

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

23.06.00

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

1999年 5月31日

REC'D 04 AUG 2000

WIPO PCT

出 願 番 号

Application Number:

平成11年特許願第152057号

09/980093

出 願 人

Applicant (s):

松下電器産業株式会社

09/980093

REC'D 04 AUG 2000

WIPO PCT

09/980093

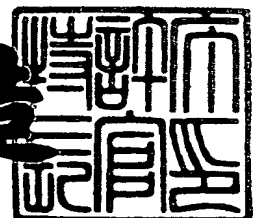
PRIORITY
DOCUMENT

SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

2000年 8月18日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2000-3064381

【書類名】 特許願

【整理番号】 2037810076

【提出日】 平成11年 5月31日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 15/78

【発明者】

 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式
会社内

 【氏名】 柏 浩

【特許出願人】

 【識別番号】 000005821

 【氏名又は名称】 松下電器産業株式会社

【代理人】

 【識別番号】 100081813

 【弁理士】

 【氏名又は名称】 早瀬 憲一

 【電話番号】 06(6380)5822

【手数料の表示】

 【予納台帳番号】 013527

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

 【包括委任状番号】 9600402

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ記録媒体、及びデータ管理システム

【特許請求の範囲】

【請求項1】 コンテンツ記録用または再生用のデータ記録媒体において、
上記データ記録媒体に、

著作権保護情報を記録し、コンテンツ再生時に該情報を参照してコンテンツの再生出力の管理を行う自立型再生履歴管理機能付き回路を具備したことを特徴とするデータ記録媒体。

【請求項2】 請求項1記載のデータ記録媒体において、

上記コンテンツは鍵を用いて暗号化されて上記ディスクメディアに記録され、

上記自立型再生履歴管理機能付き回路は、上記ディスクメディアに記録されたコンテンツを復号化するための復号鍵を記憶するとともに、上記ディスクメディアからコンテンツが再生される際に復号化されたコンテンツのデジタル形式での出力回数を制限するコンテンツ出力管理部とを有することを特徴とするデータ記録媒体。

【請求項3】 請求項2記載のデータ記録媒体において、

上記ディスクメディアに記録されたコンテンツは、タイトル単位または任意のデータサイズ単位で異なる鍵を用いて暗号化され、

上記コンテンツ出力管理部は、上記コンテンツの暗号化単位ごとの復号鍵を有し、コンテンツのタイトル単位または任意のデータサイズ単位でのデジタル形式での出力回数を制限するものであることを特徴とするデータ記録媒体。

【請求項4】 請求項2記載のデータ記録媒体において、

上記コンテンツ出力管理部は、上記コンテンツがデジタル形式で出力される際に、その回数を更新記録し、該回数を予め設定された制限回数と比較し、コンテンツのデジタル形式での出力回数が上記制限回数を超えた場合には上記コンテンツのデジタル形式での出力を抑制するものであることを特徴とするデータ記録媒体。

【請求項5】 請求項4記載のデータ記録媒体において、

上記コンテンツ出力管理部は、上記コンテンツがデジタル形式で同時に複数

の経路で出力される際に、その経路の数を記録する出力経路数記憶部を有し、コンテンツのデジタル形式での出力回数の計数時に上記出力経路数記憶部に記憶された経路の数を加味してコンテンツのデジタル形式での出力を計数するものであることを特徴とするデータ記憶媒体。

【請求項6】 請求項1記載のデータ記録媒体において、

上記コンテンツ出力管理部は、上記ディスクメディアの所有者を認識するための個人情報記憶する個人情報記憶部を有し、上記コンテンツ再生時に外部より入力された情報と上記個人情報とを比較し、比較結果が一致した場合にのみ上記コンテンツの再生を許可するものであることを特徴とするデータ記憶媒体。

【請求項7】 請求項6記載のデータ記録媒体において、

上記コンテンツ出力管理部は、外部より入力された情報と上記個人情報とを比較し、比較結果が連続して不一致になった場合に、該不一致回数を記憶する不一致回数保持部を備え、不一致回数が所定値よりも大きくなった場合には上記コンテンツの再生を抑制するとともに、外部に通知することを特徴とするデータ記憶媒体。

【請求項8】 コンテンツ記録用または再生用のデータ記録媒体を用いてデータを管理するデータ管理システムにおいて、

上記データ記録媒体に、著作権保護情報を記録し、コンテンツ再生時に該情報を参照してコンテンツの再生出力の管理を行うとともに、コンテンツ出力時に該コンテンツを所定のアルゴリズムに従って暗号化処理する自立型再生履歴管理機能付き回路を具備し、

記録再生装置に、上記自立型再生履歴管理機能付き回路と同一のアルゴリズムにて暗号化処理を行うメディア管理部を備え、

上記コンテンツ再生時に、暗号化されたコンテンツを復号化して再生することを特徴とするデータ管理システム。

【請求項9】 請求項8記載のデータ管理システムにおいて、

上記コンテンツ再生時に、上記データ記録媒体の自立型再生履歴管理機能付き回路による暗号化装置と、上記メディア管理部の暗号化処理とを用いて、データ記録媒体と上記記録再生装置との間での認証を行い、該認証結果によって上記コ

コンテンツの復号化の可否を判定することを特徴とするデータ管理システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明はデータ記録媒体、及びデータ管理システムに関し、特にデジタルコピーに対するコンテンツの著作権保護を向上させるための技術に関するものである。

【0002】

【従来の技術】

現在、コンテンツのデジタル化が進んでいるが、デジタルによるコピーは劣化が無いことから、デジタルコピーによる著作権保護が問題になっている。そのため、図44に示すように、Free、Never Copy、One More Copy、No More Copyの4つの状態により著作権保護情報を示すCGMS(Copy Generation Management System)方式が提案されている。図45はこのCGMS方式により著作権保護を制御するデジタル出力を備えた再生装置504であり、図45において、500は、例えば、CD-ROMのようなディスクメディア、504は再生装置である。そして、再生装置504は、ディスクメディアから、例えば光ピックアップなどを用いて読み出された信号を処理するための再生信号処理回路501、再生信号を出力するためのデジタルインターフェース、上記再生信号処理回路501、デジタルインターフェース503の動作を制御するためのCPU502から構成されている。

【0003】

以下、上記従来の著作権保護を制御するデジタル出力を備えた再生装置504におけるCGMS方式を用いたコンテンツのデジタル出力の制御について説明する。

まず、ディスクメディア500に付加されているCGMS情報は、再生信号処理501からCPU502に転送される。CPU502は、CGMS情報に応じてディスクメディア500の再生データの、デジタルインターフェース503からのデジタル出力を以下のように制御する。

1. CGMSが「Free」の場合は、デジタルインターフェース503からの再生データ出力を常時認める。

2. CGMSが「Never Copy」の場合は、デジタルインターフェース503からの再生データ出力を認めない。

3. CGMSが「One More Copy」の場合は、デジタルインターフェース503からの再生データ出力を1回だけ認める。

4. CGMSが「No More Copy」の場合は、デジタルインターフェース503からの再生データ出力を認めない。

【0004】

ここで、デジタルインターフェース503に記録装置が接続され、「One More Copy」のデータを記録装置に出力する場合は、記録装置側で「One More Copy」となっている情報を「No More Copy」に書き換えて記録媒体に新たにデータを記録・管理するように構成されている。

【0005】

また、上記構成では、コンテンツのCGMS情報が「One More Copy」の場合、元ディスクメディアからの1回コピーが際限なく可能であるため、これに鑑みて、コピー回数を制限するための情報をディスクメディア500面上に記録可能な管理情報領域505を設け、該情報が所定値になったらコピー禁止となるように再生装置を構成しておき、「One More Copy」のコンテンツのコピーを行う毎にコピー回数を書き換え、所定値と一致したら、それ以降の元ディスクメディアからのコピーを抑制する方式も考えられる。

【0006】

【発明が解決しようとする課題】

従来のデータ記録媒体、及びデータ管理システムは以上のように構成されており、CGMS情報を有する記録媒体から複製されたコンテンツは、これを用いてさらにコンテンツの複写を行うことができないように、記録媒体に記録時にCGMS情報の書き換えを行っているが、上記従来の構成では、例えば、CGMS情報が「One More Copy」である場合は、当該記録媒体に対するディ

デジタルコピー回数の制限ができないため、コンテンツのデジタルコピーによる著作権の侵害を効果的に防止することができないという問題点を有していた。

【0007】

また、ディスクメディアの所定領域にコピー回数を管理するための書き換え可能な領域を設けたとしても、ディスクメディアに形成されたピット形状を物理的にコピーする、いわゆる、スタンプコピーなどによる著作権の侵害を効果的に防止することができないという問題点があった。

【0008】

本発明は、上記従来の問題点を解決するためになされたものであり、ディスクメディアにおける安全性の高い著作権管理を提供することを目的とする。

【0009】

【課題を解決するための手段】

この発明の請求項1にかかるデータ記憶媒体は、コンテンツ記録用または再生用のデータ記録媒体において、上記データ記録媒体に、著作権保護情報を記録し、コンテンツ再生時に該情報を参照してコンテンツの再生出力の管理を行う自立型再生履歴管理機能付き回路を具備したものである。

【0010】

また、この発明の請求項2にかかるデータ記憶媒体は、上記請求項1記載のデータ記録媒体において、上記コンテンツは鍵を用いて暗号化されて上記ディスクメディアに記録され、上記自立型再生履歴管理機能付き回路は、上記ディスクメディアに記録されたコンテンツを復号化するための復号鍵を記憶するとともに、上記ディスクメディアからコンテンツが再生される際に復号化されたコンテンツのデジタル形式での出力回数を制限するコンテンツ出力管理部とを有するものである。

【0011】

また、この発明の請求項3にかかるデータ記憶媒体は、上記請求項2記載のデータ記録媒体において、上記ディスクメディアに記録されたコンテンツは、タイトル単位または任意のデータサイズ単位で異なる鍵を用いて暗号化され、上記コンテンツ出力管理部は、上記コンテンツの暗号化単位ごとの復号鍵を有し、コン

テンツのタイトル単位または任意のデータサイズ単位でのデジタル形式での出力回数を制限するものである。

【0012】

また、この発明の請求項4にかかるデータ記憶媒体は、上記請求項2記載のデータ記録媒体において、上記コンテンツ出力管理部は、上記コンテンツがデジタル形式で出力される際に、その回数を更新記録し、該回数を予め設定された制限回数と比較し、コンテンツのデジタル形式での出力回数が上記制限回数を超えた場合には上記コンテンツのデジタル形式での出力を抑制するものである。

【0013】

また、この発明の請求項5にかかるデータ記憶媒体は、上記請求項4記載のデータ記録媒体において、上記コンテンツ出力管理部は、上記コンテンツがデジタル形式で同時に複数の経路で出力される際に、その経路の数を記録する出力経路数記憶部を有し、コンテンツのデジタル形式での出力回数の計数時に上記出力経路数記憶部に記憶された経路の数を加味してコンテンツのデジタル形式での出力を計数するものである。

【0014】

また、この発明の請求項6にかかるデータ記憶媒体は、上記請求項1記載のデータ記録媒体において、上記コンテンツ出力管理部は、上記ディスクメディアの所有者を認識するための個人情報を記憶する個人情報記憶部を有し、上記コンテンツ再生時に外部より入力された情報と上記個人情報とを比較し、比較結果が一致した場合にのみ上記コンテンツの再生を許可するものである。

【0015】

また、この発明の請求項7にかかるデータ記憶媒体は、請求項6記載のデータ記録媒体において、上記コンテンツ出力管理部は、外部より入力された情報と上記個人情報とを比較し、比較結果が連続して不一致になった場合に、該不一致回数を記憶する不一致回数保持部を備え、不一致回数が所定値よりも大きくなった場合には上記コンテンツの再生を抑制するとともに、外部に通知するものである。

【0016】

また、この発明の請求項 8 にかかるデータ管理システムは、上記コンテンツ記録用または再生用のデータ記録媒体を用いてデータを管理するデータ管理システムにおいて、上記データ記録媒体に、著作権保護情報を記録し、コンテンツ再生時に該情報を参照してコンテンツの再生出力の管理を行うとともに、コンテンツ出力時に該コンテンツを所定のアルゴリズムに従って暗号化処理する自立型再生履歴管理機能付き回路を具備し、記録再生装置に、上記自立型再生履歴管理機能付き回路と同一のアルゴリズムにて暗号化処理を行うメディア管理部を備え、上記コンテンツ再生時に、暗号化されたコンテンツを復号化して再生するものである。

【0017】

また、この発明の請求項 9 にかかるデータ管理システムは、上記請求項 10 記載のデータ管理システムにおいて、上記コンテンツ再生時に、上記データ記録媒体の自立型再生履歴管理機能付き回路による暗号化処置と、上記メディア管理部の暗号化処理とを用いて、データ記録媒体と上記記録再生装置との間での認証を行い、該認証結果によって上記コンテンツの復号化の可否を判定するものである。

【0018】

【発明の実施の形態】

以下、本発明のよるデータ記録媒体、及びデータ管理システムについて、図面を参照しながら説明する。

実施の形態 1.

図 1 は本発明の実施の形態 1 によるデータ記録媒体であるディスクメディア 100 の概念的な構成図であり、図 1 において、90 はセンタホール、100 は、例えば、DVD-RAM などのポリカーボンで構成されたディスクメディア、101 は記憶素子として不揮発性半導体チップなどを含む半導体チップ（自立型再生履歴管理機能付き回路）、102 はデータ領域、103 はディスクメディア 100 を後述する回転ドライブに固定するためのクリッピング領域、104 はディスクメディア 100 の記録データ 102 の管理情報を記録した TOB (Table of contents) 領域である。

なおここでは、半導体チップは1個であるが、例えば2個ならばセンタホール90を挟んで対称になる様にすることで複数ある場合におけるバランスを取る様に配置してもよい。

【0019】

図2は上記ディスクメディア100に搭載された半導体チップ101と電気的な信号の接続を行うためのディスクメディアに設けられるワイヤー線の配置の一例を示した図である。図において、105はクリッピング領域103に設けられたワイヤー配線であり、ディスクメディア100の外周側から双方向の信号線であるデータ線、電源を供給する電源線、半導体チップ101駆動時のクロックを供給するクロック線、接地電位を供給するためのGND線からなり、この順で円周状に配置されている。

なお、図2ではディスクメディア100の片側上面にのみワイヤー配線を配置しているが、両面に配置するようにしてもよい。

【0020】

図3(a)，(b)は、上記構成を有するディスクメディア100を用いて記録／再生を行う記録再生装置200とディスクメディア100に設けられたワイヤー配線105との接続を行う際の一部平面図、および断面図を示し、図において106はディスクメディア100を配置するトレイ、107はディスクメディア100を固定するクリッピング、108はクリッピング107のディスクメディア100との当接面に、ディスクメディア100のワイヤー配線105に対応して設けられたワイヤー配線である。すなわち、ワイヤー配線108は、ディスクメディア100の外周側よりデータ線、電源線、クロック線、GND線が同心円上に配置されている。なお、ワイヤー配線108のうちのデータ線は、後述するメディア管理部に接続されている。

また、109はディスクメディア100を回転させるためのスピンドルモータ、208はディスクメディア100のデータ領域102に形成されたビットを読み出すための光ピックアップである。

【0021】

以上のような構成を用い、ディスクメディア100をトレイ106に搭載され

ると、トレイ 106 は記録再生装置 200 内部に収納され、ディスクメディア 100 はクリッピング 106 とスピンドルモータ 109 により上下からクランピングされ、スピンドルモータ 109 により回転し、光ピックアップ 208 によってディスクメディア 100 のデータ領域 102 をアクセスし、後述する暗号部と、記録／再生するデータの通信を行う。上記クリッピング 107 がディスクメディア 100 を固定する際に、ディスクメディア 100 に配置されたワイヤー配線が接触することでデータ線を通じて記録再生装置 200 とディスクメディア 100 上の半導体チップ 101 がデータ通信を行うことができる。

【0022】

次に動作について説明する。

まず、記録動作について説明する。

ディスクメディア 100 にコンテンツを暗号化して記録する場合、図 4 に示すように、半導体チップ 101 は、双方向の通信ポートである I/O 110、データ信号、制御信号のコントロールおよび演算を行う CPU 111（コンテンツ出力管理部）、記録データの管理情報を保持する、例えば、EPROM や EEPROM などの不揮発性メモリで構成された記憶部を有している。

【0023】

表 1 は上記記憶部 112 に保持された情報の内容を示し、114 はタイトル、115 はタイトル単位で暗号化している場合の復号鍵を保持する復号鍵部、116 はタイトル単位で、記録データのデジタル出力された回数を制限する情報であるデジタル出力制限回数情報である。

【0024】

【表 1】

114	タイトル	プログラム A . .
115	復号鍵部	鍵 A . .
116	デジタル出力 制限回数情報	5 . .

図5はディスクメディア100にデータを記録または記録データを再生するための、図3に示したところの記録再生装置200のブロック構成図であり、図5において、201は信号処理部、202はディスクメディアへのデータのリード／ライトを管理するためのメディア管理部、203は記録再生装置200におけるデータ信号、制御信号をコントロールするCPU、204は記録再生装置200と接続ケーブル213で接続された外部機器である外部記録再生装置212とのデータの双方向通信を行うためのデジタルインターフェース、205はデジタルデータをアナログに変換して出力するD/A変換器である。

【0025】

また、206はユーザが記録再生装置200の操作を行うためのユーザ設定部、207は記録再生装置200の動作を表示するユーザインターフェースでもある表示部、208はディスクメディア100にデータを記録または再生する光ピックアップ、209はアナログデータをデジタルデータに変換するA/D変換器、210は暗号部210で用いる鍵を発生する乱数部である。

【0026】

ここで、半導体チップ101のデジタル出力制限回数情報116のデータは設定しない場合は、「0」とし、設定した場合においてデジタルコピーを行う毎にカウントダウンして、その値が「1」となった場合にデジタルコピー不許可とするものとし、例えば、1回だけデジタルコピーを許可する場合には上記値を「2」に設定するものとして説明する。また、ディスクメディア100におけるコンテンツの記録または再生は、タイトル単位で行うこととする。

図6に示すように、ステップZ1、ステップZ3は記録再生装置200で行い、ステップZ2は半導体チップ101で行い、ステップZ1～ステップZ3の手順で行われる。

【0027】

すなわち、図7に示すステップZ1では、ステップA201において記録再生装置200に、ディスクメディア100を図3で示したように配置した時に、CPU203が、光ピックアップ208がディスクメディア100のTOB領域104をアクセスすることで、ディスクメディア100における、ユーザが記録し

たデータのタイトルと配置、及び空領域などを検出した上で、タイトルを表示部 207 に表示する。

【0028】

次いで、ステップ A202 において、ユーザが記録するコンテンツデータのタイトル、デジタル出力制限回数情報、コンテンツの暗号化の有無をユーザ設定部 206 に設定（ここでは、タイトル：プログラム A、デジタル出力制限回数情報：5、暗号化：有り）する。

ステップ A203 において、CPU203 はユーザ設定部 206 に設定された情報をもとに、タイトル、デジタル出力制限回数情報をメディア管理部 202 に転送し、ステップ A204 において、アナログデータであるプログラム A は、A/D 変換器 209 に入力され、ここでデジタルに変換され、さらに、信号処理部 201 に伝送され、ここでプログラム A は記録フォーマット化され、そして暗号部 210 に伝送され、暗号部 210 において、鍵を用いてプログラム A を暗号化して光ピックアップ 208 に伝送し、CPU203 の制御により光ピックアップ 208 からディスクメディア 100 の記録データ領域 102 の空領域に上記暗号化されたプログラム A を記録するとともに、記録したデータのタイトルとディスクメディア 100 におけるデータの配置を TOB 領域 104 に記録する。

ステップ A205 において、メディア管理部 202 はデータ線を介して登録コマンド、タイトル（プログラム A）、デジタル出力制限回数情報（5）、鍵 A を半導体チップ 101 に送信する。

【0029】

ステップ A2 の処理である図 8 では、ステップ A208 において、登録コマンド、タイトル（プログラム A）、デジタル出力制限回数情報（10）、鍵 A を、I/O110 で受信しする。

ステップ A209 において、CPU111 は I/O110 の受信した登録コマンドにより、ステップ A207 の受信情報を記憶部 112 に伝透し、表 1 にあるように記憶する。

そして、ステップ A210 において、記憶後通信終了をメディア管理部 202 に送信する。

ステップA3の処理である図9では、ステップA213において通信終了を受信しディスクメディア100への設定情報の記憶動作が終了する。

【0030】

以上のようにして、ディスクメディアへのコンテンツの書き込みが行われる。

次に、コンテンツを暗号化して記録しているディスクメディア100を記録再生装置200において再生する動作について図10～図14のフローチャートを参照しつつ説明する。

【0031】

図10に示すように、ステップA1、ステップA3は記録再生装置200で行い、ステップA2、ステップA4は半導体チップ101で行い、ステップA1～ステップA4の手順で行われる。

【0032】

まず、ステップA1の処理である図11では、ステップA401において、記録再生装置200にディスクメディア100を図3に示したように配置した時に、CPU203が、光ピックアップ208がディスクメディア100のTOB領域104をアクセスすることで、ディスクメディア100における、ユーザが記録したデータのタイトルと配置、及び空領域などを検出した上で、タイトルを表示部207に表示する。

【0033】

次いで、ステップA402において、ユーザ設定部206に、ユーザが再生したいタイトルをデジタルインターフェース204から接続ケーブル213を介して外部記録再生装置212に対して出力するか否かの有無を、ユーザ設定部206を介してCPU203に設定（タイトル：プログラムA、デジタル出力：有とする）する。

ステップA403において、CPU203は、再生のスタートを示すスタートコマンド、再生したいタイトル、デジタル出力の有無の情報を、メディア管理部202よりデータ線108、105を介して半導体チップ101に送信する。

【0034】

ステップA2の処理である図12では、ステップA406において、半導体チ

チップ101はステップA402で設定された情報をI/O110で受信し、CPU111がスタートコマンドを確認し、その後、ステップA407において、デジタル出力の有無を確認する。ここで、デジタル出力が無い場合（no）には、ステップA409に進んでタイトル（プログラムA）に応じて記憶部112の復号鍵部115より選択した復号鍵（鍵A）を記録再生装置200に送信する。

【0035】

一方、上記ステップA407において、デジタル出力有りの場合（yes）には、ステップA408に進んで、半導体チップ101のデジタル出力制限回数情報116と「2」とを比較してデジタル出力制限回数情報116が「2」以上の場合（yes）に、ステップA409においてタイトル（プログラムA）に応じて記憶部112の復号鍵部115より選択した復号鍵（鍵A）を記録再生装置200に送信する。

ステップA408において、デジタル出力制限回数情報116が「2」より小さい場合（no）には、ステップA410において、コンテンツを再生するための復号鍵の送信を拒否する再生不許可コマンドを記録再生装置200に送信し、ステップA411において通信を終了する。

【0036】

ステップA3の処理である図13では、ステップA414において、ステップA409における復号鍵の受信、またはステップA410における再生不許可コマンドを受信し、ステップA415において、再生不許可コマンドが確認され、再生不許可コマンドの場合（yes）に、ステップA416に進んで、表示部207において視覚または聴覚的にステップA402における設定情報の変更を促す。

【0037】

ここで、ステップA403終了以降は、ステップA402の設定情報は変更できず、変更の場合は、設定情報を消去してステップA402から設定やり直すものとする。これにより、例えば、ステップA402でデジタル出力を「無」と設定してステップA402終了後に、デジタル出力を「有り」とすることでス

チップA408よりデジタル出力が不可能なコンテンツの不正なデジタル出力を防ぐことが可能である。

【0038】

一方、上記ステップA415において、再生不許可コマンドではない場合（no）には、ステップA417に進んでステップA402で設定されたデジタル出力の有無を確認し、「有り」の場合（yes）にはステップA418に進んでステップA402で設定されたタイトル（プログラムA）のコンテンツをステップA414で受信した復号鍵（鍵）を用いて再生し、復号化データをデジタルインターフェース204よりデジタル形式で出力し、ステップA419において、再生が終了したら再生終了を半導体チップ101に送信する。

【0039】

上記ステップA417において、ステップA402で設定されたデジタル出力の有無を確認し、これが「無し」の場合（no）には、ステップA420に進んでステップA402で設定されたタイトルのコンテンツ（プログラムA）を、ステップA414で受信した復号鍵（鍵A）を用いて復号化してD/A変換器205からのアナログ形式で再生する。

【0040】

ステップA4の処理である図14では、ステップA422において半導体チップ101は再生終了をI/O110で受信し、CPU111が再生終了を確認したらステップA423において記憶部112のデジタル出力制限回数情報116から「1」を引いた回数「5-1=4」をデジタル出力制限回数情報116を更新することで記録してコンテンツの再生が終了する。

【0041】

以上のように、本実施の形態によれば、コンテンツ記録媒体であるディスクメディア100に半導体チップ101を設け、半導体チップ101にデジタル出力回数を制限するための情報を保持させて管理するようにしたので、コンテンツのデジタルコピー等のデジタル出力の回数を制限でき、また、スタンプコピーのような方法で物理的にコンテンツ記憶領域をコピーしても、半導体チップ101はコピーされず、しかもコンテンツは半導体チップ101内に格納された鍵

でしか符号化できないように暗号化されているので、コンテンツの内容が再生可能な状態で外部に取り出されることがない。

【0042】

さらに、ステップA423においてコンテンツの再生終了を確認した上で、デジタル出力制限回数情報を更新するようにしているため、何らかのトラブルなどで再生途中でデジタル出力が停止した場合においても、コンテンツのデジタル出力を保証することができる。

【0043】

実施の形態2.

次に本発明の実施の形態2によるデータ記録媒体、及びデータ管理システムについて説明する。上記実施の形態1では、デジタルインターフェースが1つである場合について説明したが、本実施の形態2では、複数のデジタル入出力口を備えた再生動作を用いる場合について説明する。

【0044】

図15は半導体チップ101aの構成を示す図であり、図において、113は記録データを再生する装置の外部にデジタル出力する場合に、外部にデジタル出力する数を保持するためのデジタル出力数保持部（出力経路数記憶部）である。ここで、その他、図4と同一符号は同一または相当部分を示すものとする。

【0045】

図16は複数のデジタル入出力口備え、ディスクメディア100の記録データを再生可能な図3における動作を保有する記録再生装置のブロック図であり、図において、300は記録再生装置、301はデジタルインターフェース（A）、302は複数のデジタル出力口を有するデジタルインターフェース（B）、303はハードディスク（HDD）装置（A）、304はハードディスク（HDD）装置（B）である。その他、図5と同一符号は同一または相当部分を示すものとする。

【0046】

以上に構成された再生装置400について図18～21のフローチャートを参

照しつつ説明する。

ディスクメディア100におけるコンテンツを再生するには、図17に示すように、ステップB1とステップB3は記録再生装置300で行い、ステップB2とステップB4を半導体チップ101aで行い、ステップB1～ステップB4の手順で行う。

【0047】

ステップB1の処理である図18では、ステップA601において、記録再生装置400にディスクメディア100を図3のように配置した時に、CPU203は光ピックアップ208がTOB領域104をアクセスすることで、ディスクメディア100における、ユーザが記録したデータのタイトルと配置、および空領域等を認識した上で、タイトルを表示部207に表示する。

【0048】

次いで、ステップB602において、ユーザ設定部206にユーザが再生したいタイトルをデジタルインターフェースA301、302から、接続ケーブル213を介して外部記録再生装置212、HDD装置A303、B304に対してデジタル出力する場合に選択し、デジタル出力する数をユーザ設定部206を介してCPU203に設定（タイトル：プログラムA、デジタル出力：3とする）し、ステップB603において、再生のスタートを示すスタートコマンド、再生したいタイトル、デジタル出力の数を半導体チップ101に透信する。ここで、ステップB602におけるデジタル出力がない場合は「0」として説明する。

【0049】

ステップB2の処理である図19では、ステップB606において、ステップB602で設定された情報を受信し、スタートコマンドを確認した後、ステップB607においてデジタル出力数を「1」と比較することで、デジタル出力の有無を検出している。そして、ステップB607において、デジタル出力数が「0」の場合（no）には、デジタル出力を「無い」としてステップB614に進んで、タイトルに応じて復号鍵部115より選択した復号鍵（鍵A）を記録再生装置300に送信する。

一方、ステップB607においてデジタル出力数が「0」以外の場合（yes）には、デジタル出力を「有り」としてステップB608に進んでデジタル出力制限回数情報116と「2」とを比較することでデジタル出力が可能かを検出する。

【0050】

次いで、ステップB608において、デジタル出力制限回数情報107が「2」より小さい場合（no）には、ステップB611に進んで、コンテンツを再生するための復号鍵の送信を拒否する再生不許可コマンドを半導体チップ101に送信する。一方、上記ステップB608において、デジタル出力制限回数情報116が「2」以上の場合（yes）にはステップB609を実行する。

【0051】

上記ステップB609においては、デジタル出力数と「2」とを比較して、デジタル出力数が「2」未満、つまり、「1」以下の場合（no）には、ステップB613においてデジタル出力数をデジタル出力数保持部113に設定し、ステップB614においてタイトル（プログラムA）に応じて復号鍵部115より選択した復号鍵（鍵A）を記録再生装置300に送信する。

【0052】

上記ステップB609においてデジタル出力数が2より大きい場合（yes）にはステップB610に進んで、ここで、デジタル出力制限回数情報116ーデジタル出力数と、「2」とを比較して、デジタル出力制限回数情報116ーデジタル出力数が「2」よりも小さい場合（yes）にステップB611においてコンテンツを再生するための復号鍵の送信を拒否する再生不許可コマンドを半導体チップ101に送信し、ステップB612において通信を終了する。

【0053】

一方、上記ステップB610においてデジタル出力制限回数情報116ーデジタル出力数が「1」以上の場合（no）には、ステップB613に進んでデジタル出力数をデジタル出力数保持部113（3）に設定し、ステップB614においてタイトル（プログラムA）に応じて復号鍵115より選択した復号鍵（鍵A）を記録再生装置300に送信する。

【0054】

ステップB3の処理である図20では、ステップB616において、ステップB611の再生不許可コマンド、またはステップB614の復号鍵を受信し、ステップB617において、上記受信したものが再生不許可コマンドか否かを確認し、これが再生不許可コマンドであった場合（yes）には、ステップB619に進んで、表示部207において視覚または聴覚的にステップB602における設定情報の変更を促す。

【0055】

一方、上記ステップB617において、受信したものが再生不許可コマンドでないと判定された場合（no）には、ステップB620に進んで、デジタル出力数と「1」とを比較することで、デジタル出力の有無を検出する。

ステップB620において、デジタル出力数が「1」の場合（no）には、デジタル出力を「無い」としてステップB623において、ステップB602で設定されたタイトル（プログラムA）のコンテンツをステップB616で受信した復号鍵（鍵A）を用いてD/A変換器205からのアナログ出力のみを再生する。

【0056】

一方、上記ステップB620において、デジタル出力数が「1」以外の場合（yes）には、デジタル出力を「有り」として、ステップB602で設定されたタイトル（プログラムA）のコンテンツを、ステップB616で受信した復号鍵（鍵A）を用いて再生し、デジタルインターフェース（A）301、またはデジタルインターフェース（B）302よりデジタル形式で出力し、ステップB622において再生が終了したら再生終了を半導体チップ101aに送信する。

【0057】

ステップB4の処理である図21では、ステップB625において、再生終了の確認行い、再生終了ならばステップB626に進んで、デジタル出力制限回数情報116からデジタル出力数保持部113（3）を引いた回数をデジタル出力制限回数情報116（2）を更新することで記憶させ、コンテンツの再生

を終了する。

【0058】

このように本実施の形態2によれば、複数のデジタル出力口を備えた再生装置において、半導体チップ101aに、デジタル出力する数を保持する機能を持たせ、デジタルコピー終了後に、デジタル出力制限回数情報116からデジタル出力数保持部113の値を減算することで、複数のデジタル出力を用いて、再生したコンテンツを同時にデジタルコピー等する場合におけるコピー回数の制限を行うことができる。

【0059】

実施の形態3.

次に本発明の実施の形態3によるデータ記録媒体、及びデータ管理システムについて説明する。本実施の形態3では、上記実施の形態1または2において、半導体チップ101bが、ユーザの個人情報（パスワード）を用いた本人認証することでディスクメディアの再生を許可する機能を付加したものである。なお、ここでは、実施の形態1に本実施の形態3の機能を適用したものを例にとって説明する。

【0060】

図22は本実施の形態3における半導体チップ101bの構成を示すブロック図であり、図において、117は本人認証を目的とするパスワードを保持する個人情報保持部（個人情報記憶部）である。その他の部分については、図4と同一であるのでここでは、その説明については省略するものとする。

【0061】

以上のように構成された本実施の形態3の動作について図23～27のフローチャートを参照しつつ説明する。なお、ここでは、個人情報保持部117が「0」の値の場合に個人情報が登録されていないものとし、ディスクメディア100は記録または再生しようとする装置に配置され、電源が投入された時点で、半導体チップ101bのCPU111が個人情報保持部117を確認し、個人情報が設定（0以外に）されている場合に、記録再生装置200からの入力された個人情報と一致しなければ記憶部112へのアクセスを制限するものとして説明する。

【0062】

まず、本人を認証するための個人情報を半導体チップ101に記録再生装置200によって登録する動作について説明する。

図23に示すように、ステップC1、ステップC3は記録再生装置200で行い、ステップC2とステップC4を半導体チップ101bで行い、ステップC1～ステップC5の手順で行う。

ステップC1の処理である図24では、ステップC801において、ディスクメディア100が記録再生装置200に配置されることで、CPU203はディスクメディア100における個人情報の登録の有無を確認する個人情報確認コマンドを送信する。

【0063】

次いで、ステップC2の処理である図25では、ステップC804において、個人情報確認コマンドを受信し、CPU111bは個人情報確認コマンドに基づきステップD805において個人情報の有無を確認するために、個人情報保持部117と「0」とを比較して個人情報保持部117が「0」の場合（no）には、「個人情報無し」としてステップC807に進んで個人情報無しコマンドを送信する。一方、上記ステップC805において個人情報保持部117が「0」では無い場合（yes）には、「個人情報有り」としてステップC806に進んで個人情報有りコマンドを送信する。

【0064】

ステップC3の処理である図26では、ステップC811において個人情報有りコマンド、または個人情報無しコマンドを受信し、CPU203はステップC812において、個人情報無しコマンドか否かを確認し、個人情報が無しコマンドが検出された場合（yes）には、ステップC813に進んで再生動作を行うか、または個人情報を登録するための登録コマンドと登録する個人情報をユーザ設定部206より入力して半導体チップ101bに送信する。なお、上記ステップC812において個人情報が無しコマンド以外が検出された場合（no）の動作については後述するの本人認証の動作で説明する。

ステップC4の処理である図27では、ステップC817において登録コマンドと登録する個人情報を受信し、CPU111bは登録コマンドに基づき、ステップC818において個人情報を個人情報保持部117に記憶する。

【0065】

次に本人認証を行うための個人情報が半導体チップ101bに登録されている場合における、記録再生装置200の動作を図28～31を参照しつつ説明する。

図28に示すように、ステップC1とステップD3とステップD5は記録再生装置200で行い、ステップC2とステップD4を半導体チップ101bで行い、ステップD1～ステップD5の手順で行う。なおここでは、図23～27と同一ステップ名は同一処理としてその説明を省略するものとする。

【0066】

ステップD3の処理である図29では、ステップD1011において個人情報有りコマンド、または個人情報無しコマンドを受信し、次いで、CPU203はステップD1012において、個人情報無しコマンドか否かを確認し、個人情報が無しコマンド以外の場合（no）には、ステップD1014において表示部207に個人情報の入力を促し、個人情報が入力された時点でステップD1015において、個人情報の確認命令である個人情報コマンドと入力個人情報とを半導体チップ101bに送信する。

【0067】

次いで、ステップD4の処理である図30では、ステップD1018において、個人情報コマンドと入力個人情報とを受信し、CPU111bは個人情報コマンドに基づいてステップD1019において、個人情報保持部117と入力個人情報とを比較し、これらが一致した場合（yes）には、ステップD1020に進んで本人認証成立を伝える継続コマンドを送信し、逆に、不一致の場合（no）にはステップD1021に進んで通信終了を送信する。

【0068】

ここで、ステップD1019において（yes）の場合にユーザの本人認証が成立し、CPU111bは、以後、記憶部112へアクセスを行うように動作することで、ディスクメディア100への記録または再生動作が可能になる。

【0069】

ステップD5の処理である図31では、ステップD1024において継続コマンド、または通信終了を受信し、ステップD1025においてCPU203は継続コマンドか否かの確認を行い、ここで継続コマンドの場合（yes）であると判定された場合には、ステップD1026に進んで、ディスクメディア100への記録または再生動作や、個人情報保持部117の情報を消去するための命令である消去コマンドの発行や、登録されている個人情報を変更するための登録コマンド等を送信することが可能となる。

【0070】

一方、上記ステップD1025において、継続コマンドでないと判定された場合（no）には、ステップD1027に進んで通信を終了する。

【0071】

なお、上記個人情報保持部117に、複数の個人情報を備え、ユーザが個人情報保持部117の自分の個人情報を選択し、上記動作を複数回行うように構成することも可能である。

また、半導体チップ101bの記憶部112に登録しているタイトル単位で本人認証情報を設定し、本人認証が成立したときのみ再生可能となるように構成してもよい。

【0072】

このように本実施の形態3によれば、ディスクメディア100の半導体チップ101bに、ユーザの個人情報（パスワード）を記憶し、メディア再生時に認証を行うようにすることで、ディスクメディア側でユーザの識別が可能となり、第三者によるディスクメディア100の不正コピー等の行為を防止することができ、コンテンツの安全性を強固なものとすることができる。

【0073】

実施の形態4.

次に本発明の実施の形態4によるデータ記録媒体、及びデータ管理システムについて説明する。本実施の形態4では、上記実施の形態3において、半導体チップの個人情報保持部に個人情報が設定されている場合、本人認証への不正動作を

検出する機能を付加したものである。すなわち、図 3 2 は本実施の形態 4 における半導体チップ 1 0 1 c の構成を示すブロック図であり、図において、1 1 8 は個人情報（パスワード）の確認が一致しなかった回数を保持するための不正回数保持部（不一致回数保持部）である。その他の部分については図 2 2 で示したものと同一であるので、ここではその説明は省略する。

なお、ここでは、不正回数保持部 1 1 8 には「0」以外の任意の値が設定されており、記憶された値をクリアすることで任意の値が設定されるものとし、不正回数保持部 1 1 8 に「0」が保持されると不正アクセスが検出されたものとして説明する。

【0074】

以下、本人認証するための個人情報が半導体チップ 1 0 1 c に登録されている場合に、例えば、個人情報を解析する目的など、不正なアクセスを検出する動作を中心に、図 3 3 から 3 5 を参照しつつ説明する。

図 3 3 に示すように、ステップ C 1 とステップ D 3 とステップ E 5 は記録再生装置 2 0 0 で行い、ステップ C 2 とステップ E 4 を半導体チップ 1 0 1 で行い、ステップ D 1 ～ステップ E 5 の手順で行う。ここで、図 2 8 と同一ステップ名は同一処理としてその説明は省略する。

【0075】

まず、ステップ E 4 の処理である図 3 4 では、ステップ E 1 1 0 1 において、個人情報コマンドと入力個人情報とを受信する。

次いで、CPU 1 1 1 c は、ステップ E 1 1 0 2 において、不正回数保持部 1 1 8 の記憶内容と「0」とを比較し、不正回数保持部 1 1 8 の記憶内容が「0」の場合（y e s）には、ステップ E 1 1 0 3 に進んで不正行為があったとして不正アクセスコマンドを記録再生装置 2 0 0 に送信する。

【0076】

一方、上記ステップ E 1 1 0 2 において、不正回数保持部 1 1 8 の記憶内容が「0」以外の場合（n o）には、ステップ E 1 1 0 4 に進んで、CPU 1 1 1 c は個人情報コマンドに基づいて、個人情報保持部 1 1 7 と入力個人情報とを比較し、その結果が一致した場合（y e s）には、ステップ E 1 1 0 5 に進んで不正

回数保持部 118 をクリアして「0」以外の所定値を設定し、ステップ E 1106 において、本人認証成立を伝える継続コマンドを送信する。一方、上記ステップ E 1104 において、不一致の場合 (no) にはステップ E 1107 に進んで不正回数保持部 118 に記憶された値から「1」を減算した結果を不正回数保持部 118 として保持し、ステップ E 1108 において通信終了を記録再生装置 200 に送信する。

【0077】

上記ステップ E 1105 を実行することで、不正回数保持部 118 に設定されている値が「0」になる前に本人認証が成立すれば、不正回数保持部 118 がクリアされて所定値にもどる。これにより本人の誤入力などによって不正回数が記録しても、再度、正しい入力を行うことで上記誤入力による不正回数がカウントされ、誤入力による不正回数の蓄積によって不意にディスクメディアへのアクセスが不可能になることを防止している。また、本人以外の人物が不正な本人認証をしようと個人情報保持部 117 に記憶されていない情報を連続し入力した場合には、不正回数保持部 118 の値が「0」に近づいていき、不正回数保持部 118 が「0」になったときに不正アクセスがあったことが検出できる。

【0078】

ステップ E 5 の処理である図 35 では、ステップ E 1111 において、不正アクセスコマンド、または継続コマンド、または通信終了のいずれかを受信し、ステップ E 1112 において、CPU 203 は、上記受信した情報が、不正アクセスコマンドか否かの確認を行い、不正アクセスコマンドであった場合 (yes) には、ステップ E 1113 に進んで表示部 207 において視覚、または聴覚的に不正行為があったことの表示を行う。

【0079】

一方、上記ステップ E 1112 において、上記 CPU 203 が不正アクセスコマンド以外の情報を確認した場合 (no) には、ステップ D 1114 に進んで CPU 203 は、その情報が継続コマンドか否かの確認をし、これが継続コマンドである場合 (yes) には、ステップ E 1115 に進んでディスクメディア 100 への記録または再生動作、個人情報保持部 117 の情報を消去するための命令

である消去コマンドの発行、登録されている個人情報を変更するための登録コマンド等を送信することができる。

上記ステップ E1114 において、CPU203 が、継続コマンドでないと判定した場合 (no) には、ステップ E1116 に進んで通信を終了する。

【0080】

このように本実施の形態 4 によれば、ディスクメディア 100 の半導体チップ 101c に不正アクセスした回数を記憶する機能を設けることで、例えば、第 3 者が悪意でディスクメディア 100 に不正アクセスしたことをディスクメディア 100 側で記録保持することができるため、ディスクメディア 100 の正規の所有者に不正アクセスがあったことを警告することができる。

また、不正アクセスを検出した場合に、再生装置が、例えば、大きな音を発するなど威嚇して不正行為を止めさせることも可能である。

【0081】

実施の形態 5.

次に本発明の実施の形態 5 によるデータ記録媒体、及びデータ管理システムについて説明する。本実施の形態 5 では、上述した各実施の形態において、暗号を用いた認証動作を行うようにしたものである。なお、ここでは実施の形態 1 において適用した場合を例にとって説明する。

図 36 は本実施の形態 5 における半導体 IC101d の構成を示すブロック図であり、図において、119 は記録再生装置 200 の暗号部 210 と同じ暗号アルゴリズムを有する暗号部、120 は乱数を発生する乱数部、121 はの暗号部 120 で用いる鍵配列の集合である鍵ボックス部である。その他の部分については、図 4 で示したものと同一であるため、ここではその説明は省略する。図 37 は本実施の形態 5 における記録再生装置 400 のブロック図であり、図 37 において、214 はディスクメディア 100 に搭載された半導体チップ 101d に含まれる鍵ボックス部 121 と同一機能を有する鍵ボックス部である。その他、図 5 と同一符号は同一または相当部分を示す。

表 2 は上記鍵ボックス部 121、鍵ボックス部 214 に保持されている情報であり、表 2 において、1700 は鍵を選択するための鍵コード、1701 は鍵コ

ード 1 7 0 0 に応じて選択される鍵である。

【表 2】

1700 鍵コード	1701 鍵
鍵コード1	鍵KC1
鍵コード2	鍵KC2
⋮	⋮

以上に構成されたディスクメディア 1 0 0 の半導体チップ 1 0 1 d と記録再生装置 4 0 0 における認証動作について図 3 8 ～ 4 1 のフローチャートを参照しつつ説明する。図 3 8 に示すように、ステップ G 1、ステップ G 3、ステップ G 5 は記録再生装置 4 0 0 で行い、ステップ C 2、ステップ G 4 を半導体チップ 1 0 1 で行いステップ G 1 ～ ステップ G 5 の手順で行う。

【0 0 8 2】

また、以降データの暗号化、または復号化においては下記のように示すものとする。

$$\text{関数名} = E / D (A, B)$$

$E / D = E$: 暗号化、 D = 復号化とし、 A は暗号化または復号化における鍵、 B は平文または暗号文を示している。

例えば、平文 B を鍵 A により暗号化して暗号文 C を生成するには、

$$C = E (A, B)$$

とする。復号化は、

$$B = D (A, C)$$

ステップ G 1 の処理である図 3 9 では、ステップ G 1 8 0 1 において認証スタートコマンドを半導体チップ 1 0 1 d に送信する。

【0 0 8 3】

ステップ G 2 の処理である図 4 0 では、ステップ G 1 8 0 4 において認証スタートコマンドを受信し、CPU 1 1 1 d は認証スタートコマンドに基づいてステ

ップG1805において乱数部120により乱数を発生し、乱数RXとし、ステップG1806において乱数RXの並びを利用して、「鍵コード1」を生成し、鍵ボックス部121で鍵を選択して「鍵KC1」とし、ステップG1807において乱数RXを「鍵KC1」を鍵として暗号部120で暗号化： $E1 = E(KC1, RX)$ を実行しE1を作成し、ステップG1809においてE1と「鍵コード1」を記録再生装置400に送信する。

【0084】

ステップG3の処理である図41では、ステップG1810においてE1と「鍵コード1」を受信し、CPU203はステップG1811において、鍵ボックス部214で「鍵コード1」に対応した「鍵KC1」を選択し、ステップG1812において、E1を「鍵KC1」を鍵として暗号部1600で復号化： $D1 = D(KC1, E1)$ を実行してD1を作成する。

【0085】

次いで、ステップG1814において、乱数部211で乱数を発生し、乱数の並びを利用して「鍵コード1」とは異なる「鍵コード2」を生成し、ステップG1815において「鍵コード2」により鍵ボックス部214から鍵を選択し「鍵KC2」とし、ステップG1816においてD1を「鍵KC2」を鍵として暗号部210で暗号化： $E2 = (KC2, D1)$ してE2を作成し、ステップG1817において、E2と「鍵コード2」を半導体チップ101dに送信し、ステップG1818においてD1と「鍵KC1」と「鍵KC2」を排他的論理和 $KI1 = D1 \wedge KC1 \wedge KC2$ （ \wedge は排他的論理和をあらわす記号とする）して記録、または再生に必要なデータを暗号化伝送するための鍵として用いる伝送鍵である「KI1」を作成する。

【0086】

ステップG4の処理である図42では、ステップG1821において、E2と「鍵コード2」を受信し、CPU111dはステップG1822において、鍵ボックス部121で「鍵コード2」に対応した「鍵KC2」を選択し、ステップG1823においてE2を「鍵KC2」を鍵として暗号部120で復号化： $D2 = (KC2, E2)$ を実行してD2を作成し、ステップG1824において、乱数

RXとD2を比較して、乱数RXとE2が不一致の場合（no）には、ステップG1827に進んで通信終了を送信し、ステップG1828において通信終了する。

【0087】

一方、上記ステップG1824において乱数RXとE2が一致した場合（yes）には、半導体チップ101dは記録再生装置400を認証し、ステップG1825においてRXと「鍵KC1」と「鍵KC2」を排他的論理和 $K12 = RX \oplus KC1 \oplus KC2$ として記録、または再生に必要なデータを暗号化伝送するための鍵として用いる伝送鍵である「KI2」を作成し、ステップG1825において継続コマンドを送信する。

【0088】

ステップG1の処理である図43では、ステップG1531において、継続コマンド、または通信終了を受信し、ステップG1532において、上記受信した情報が継続コマンドか否かを確認し、これが継続コマンドではないと判定された場合（no）には、ステップG1534に進んで通信終了し、逆に、継続コマンドであると判定された場合（yes）には、ステップG1503に進んで再生動作を行う。

【0089】

このように本実施の形態5によれば、ディスクメディア100の半導体チップ101dに暗号処理機能を設け、暗号を用いて認証を行うようにしたので、暗号通信可能な環境下でのみディスクメディアの再生が許可されることとなり、より、コンテンツのセキュリティを高めることができる。

さらに、ステップG1818およびステップ1825において、乱数データを合む通信過程のデータを用いて、記録または再生動作に必要なデータを暗号化して伝送するための伝送鍵を認証ごとに異ように生成するので、安全性の高い鍵を作成できる。

【0090】

なお、上記実施の形態1では、ディスクメディア100に搭載される半導体チップ101に電源や信号を供給するのに、クリッピング領域103にワイヤー配

線 105 を用いて行う例を示したが、例えば、クリッピング領域に太陽電池パネルを搭載し、これによって半導体チップに電源を供給するとともに、半導体レーザを太陽電池パネルの特定位置に照射することで、信号のやり取りを行うような構成とすることも可能である。

【0091】

また、上記実施の形態 3 では、ディスクメディアに個人情報としてパスワードを保持さ、これを確認させたり、実施の形態 5 では、暗号処理を用いてディスクメディアと再生装置との間での認証を行うようにしたが、認証にかかるアルゴリズムを IC カードなどの媒体に持たせ、IC カードなどの媒体をコンテンツ再生時に鍵代わりに用いるようにすることで、不正利用を防止するようにすることも可能である。

【0092】

さらに、上記各実施の形態では、コンテンツを記録する媒体として、ディスクメディアを例にとって説明したが、他にも、HDD やテープや、ROM などについても、これらに記録されたコンテンツの再生を管理する半導体チップを具備することで、上記各実施の形態と同様の効果を得ることができる。

【0093】

【発明の効果】

以上のように、この発明の請求項 1 にかかるデータ記憶媒体によれば、コンテンツ記録用または再生用のデータ記録媒体において、上記データ記録媒体に、著作権保護情報を記録し、コンテンツ再生時に該情報を参照してコンテンツの再生出力の管理を行う自立型再生履歴管理機能付き回路を具備したものとしたので、コンテンツの再生を自己で管理することができ、コピー元の記録媒体を用いた無制限な複製を防止することができ、著作権の侵害を効果的に防止することができるという効果が得られる。

【0094】

また、この発明の請求項 2 にかかるデータ記憶媒体によれば、上記請求項 1 記載のデータ記録媒体において、上記コンテンツは鍵を用いて暗号化されて上記ディスクメディアに記録され、上記自立型再生履歴管理機能付き回路は、上記ディ

スクメディアに記録されたコンテンツを復号化するための復号鍵を記憶するとともに、上記ディスクメディアからコンテンツが再生される際に復号化されたコンテンツのデジタル形式での出力回数を制限するコンテンツ出力管理部とを有するものとしたので、や、物理的なスタンプコピーなどを行ってもコンテンツが暗号化されているために、再生することができず、著作権の侵害を効果的に防止することができるという効果が得られる。

【0095】

また、この発明の請求項3にかかるデータ記憶媒体によれば、上記請求項2記載のデータ記録媒体において、上記ディスクメディアに記録されたコンテンツは、タイトル単位または任意のデータサイズ単位で異なる鍵を用いて暗号化され、上記コンテンツ出力管理部は、上記コンテンツの暗号化単位ごとの復号鍵を有し、コンテンツのタイトル単位または任意のデータサイズ単位でのデジタル形式での出力回数を制限するようにしたので、コンテンツの著作権をより強固なものとすることができるという効果が得られる。

【0096】

また、この発明の請求項4にかかるデータ記憶媒体によれば、上記請求項2記載のデータ記録媒体において、上記コンテンツ出力管理部は、上記コンテンツがデジタル形式で出力される際に、その回数を更新記録し、該回数を予め設定された制限回数と比較し、コンテンツのデジタル形式での出力回数が上記制限回数を超えた場合には上記コンテンツのデジタル形式での出力を抑制するようにしたので、コンテンツのデジタル形式での複製回数を制限することができるという効果が得られる。

【0097】

また、この発明の請求項5にかかるデータ記憶媒体によれば、上記請求項4記載のデータ記録媒体において、上記コンテンツ出力管理部は、上記コンテンツがデジタル形式で同時に複数の経路で出力される際に、その経路の数を記録する出力経路数記憶部を有し、コンテンツのデジタル形式での出力回数の計数時に上記出力経路数記憶部に記憶された経路の数を加味してコンテンツのデジタル形式での出力を計数するようにしたので、デジタル形式の出力インターフェイ

スを複数個備えた再生装置においても、複製回数を管理することができるという効果がある。

【0098】

また、この発明の請求項6にかかるデータ記憶媒体によれば、上記請求項1記載のデータ記録媒体において、上記コンテンツ出力管理部は、上記ディスクメディアの所有者を認識するための個人情報を記憶する個人情報記憶部を有し、上記コンテンツ再生時に外部より入力された情報と上記個人情報とを比較し、比較結果が一致した場合にのみ上記コンテンツの再生を許可するようにしたので、データ記憶媒体の所有者以外の不特定な人物がコンテンツを無許可で再生することを防止することができるという効果が得られる。

【0099】

また、この発明の請求項7にかかるデータ記憶媒体は、請求項6記載のデータ記録媒体において、上記コンテンツ出力管理部は、外部より入力された情報と上記個人情報とを比較し、比較結果が連続して不一致になった場合に、該不一致回数を記憶する不一致回数保持部を備え、不一致回数が所定値よりも大きくなった場合には上記コンテンツの再生を抑制するとともに、外部に通知するものである。

【0100】

また、この発明の請求項8にかかるデータ管理システムは、上記コンテンツ記録用または再生用のデータ記録媒体を用いてデータを管理するデータ管理システムにおいて、上記データ記録媒体に、著作権保護情報を記録し、コンテンツ再生時に該情報を参照してコンテンツの再生出力の管理を行うとともに、コンテンツ出力時に該コンテンツを所定のアルゴリズムに従って暗号化処理する自立型再生履歴管理機能付き回路を具備し、記録再生装置に、上記自立型再生履歴管理機能付き回路と同一のアルゴリズムにて暗号化処理を行うメディア管理部を備え、上記コンテンツ再生時に、暗号化されたコンテンツを復号化して再生するようにしたので、コンテンツの著作権を効果的に保護することができるという効果が得られる。

【0101】

また、この発明の請求項9にかかるデータ管理システムは、上記請求項8記載のデータ管理システムにおいて、上記コンテンツ再生時に、上記データ記録媒体の自立型再生履歴管理機能付き回路による暗号化処理と、上記メディア管理部の暗号化処理とを用いて、データ記録媒体と上記記録再生装置との間での認証を行い、該認証結果によって上記コンテンツの復号化の可否を判定するようにしたので、データ記録媒体と記録再生装置との間で認証を行うことができ、コンテンツの著作権の保護をさらに強固なものとすることができるという効果が得られる。

【図面の簡単な説明】

【図1】 本発明の実施の形態1によるデータ記憶媒体であるディスクメディアの概念的な構成を示す図である。

【図2】 上記実施の形態1のディスクメディアのワイヤー配線を含む構成を示す図である。

【図3】 上記実施の形態1のディスクメディアに記録されたコンテンツを再生もしくは、コンテンツを記録する際に使用する記録再生装置と上記ディスクメディアの配置を示す図(a)、及びディスクメディアを回転させるためのモータに載置した状態を示す図(b)である。

【図4】 上記実施の形態1の半導体チップの構成を模式的に示す構成図である。

【図5】 上記実施の形態1によるデータ記憶媒体を用いたデータ管理システムの全体的な構成を示す構成図である。

【図6】 上記実施の形態1によるデータ管理システムを用いてコンテンツを暗号化して記録する際の全体的な動作を示す図である。

【図7】 上記実施の形態1によるデータ管理システムの記録時のステップZ1の詳細な工程を示す図である。

【図8】 上記実施の形態1によるデータ管理システムのステップZ2の記録時の詳細な工程を示す図である。

【図9】 上記実施の形態1によるデータ管理システムのステップZ3の記録時の詳細な工程を示す図である。

【図10】 本発明実施の形態1によるディスクメディアに記録されたコン

テンツを記録再生装置によって再生する際の全体的な動作を説明するための図である。

【図 1 1】 上記実施の形態 1 によるデータ管理システムのコンテンツを再生する際のステップ A 1 の詳細な工程を示す図である。

【図 1 2】 上記実施の形態 1 によるデータ管理システムのコンテンツを再生する際のステップ A 2 の詳細な工程を示す図である。

【図 1 3】 上記実施の形態 1 によるデータ管理システムのコンテンツを再生する際のステップ A 3 の詳細な工程を示す図である。

【図 1 4】 上記実施の形態 1 によるデータ管理システムのコンテンツを再生する際のステップ A 4 の詳細な工程を示す図である。

【図 1 5】 本発明の実施の形態 2 によるデータ記憶媒体であるディスクメディアに搭載された半導体チップの構成を模式的に示す構成図である。

【図 1 6】 上記実施の形態 2 によるデータ記憶媒体を用いたデータ管理システムの全体的な構成を示す構成図である。

【図 1 7】 本発明実施の形態 2 によるディスクメディアに記録されたコンテンツを記録再生装置によって再生する際の全体的な動作を説明するための図である。

【図 1 8】 上記実施の形態 2 によるデータ管理システムのコンテンツを再生する際のステップ B 1 の詳細な工程を示す図である。

【図 1 9】 上記実施の形態 2 によるデータ管理システムのコンテンツを再生する際のステップ B 2 の詳細な工程を示す図である。

【図 2 0】 上記実施の形態 2 によるデータ管理システムのコンテンツを再生する際のステップ B 3 の詳細な工程を示す図である。

【図 2 1】 上記実施の形態 2 によるデータ管理システムのコンテンツを再生する際のステップ B 4 の詳細な工程を示す図である。

【図 2 2】 本発明の実施の形態 3 によるデータ記憶媒体であるディスクメディアに搭載された半導体チップの構成を模式的に示す構成図である。

【図 2 3】 上記実施の形態 3 によるデータ記憶媒体を用いたデータ管理システムの個人情報を登録する手順を示す全体的な構成図である。

【図 2 4】 上記実施の形態 3 によるデータ管理システムの個人情報を登録する手順であるステップ C 1 の詳細な工程を示す図である。

【図 2 5】 上記実施の形態 3 によるデータ管理システムの個人情報を登録する手順であるステップ C 2 の詳細な工程を示す図である。

【図 2 6】 上記実施の形態 3 によるデータ管理システムの個人情報を登録する手順であるステップ C 3 の詳細な工程を示す図である。

【図 2 7】 上記実施の形態 3 によるデータ管理システムの個人情報を登録する手順であるステップ C 4 の詳細な工程を示す図である。

【図 2 8】 上記実施の形態 3 によるデータ記憶媒体を用いたデータ管理システムの登録された個人情報を確認するための手順を示す全体的な構成図である。

【図 2 9】 上記実施の形態 3 によるデータ管理システムの登録された個人情報を確認するための手順であるステップ D 3 の詳細な工程を示す図である。

【図 3 0】 上記実施の形態 3 によるデータ管理システムの登録された個人情報を確認するための手順であるステップ D 4 の詳細な工程を示す図である。

【図 3 1】 上記実施の形態 3 によるデータ管理システムの登録された個人情報を確認するための手順であるステップ D 5 の詳細な工程を示す図である。

【図 3 2】 本発明の実施の形態 4 によるデータ記憶媒体であるディスクメディアに搭載された半導体チップの構成を模式的に示す構成図である。

【図 3 3】 上記実施の形態 4 によるデータ記憶媒体を用いたデータ管理システムの個人情報確認時の不正アクセスを記録するための手順を示す全体的な構成図である。

【図 3 4】 上記実施の形態 4 によるデータ管理システムの不正アクセスを記録する手順であるステップ E 4 の詳細な工程を示す図である。

【図 3 5】 上記実施の形態 4 によるデータ管理システムの不正アクセスを記録する手順であるステップ E 5 の詳細な工程を示す図である。

【図 3 6】 本発明の実施の形態 5 によるデータ記憶媒体であるディスクメディアに搭載された半導体チップの構成を模式的に示す構成図である。

【図 3 7】 上記実施の形態 5 によるデータ記憶媒体を用いたデータ管理シ

システムの全体的な構成を示す構成図である。

【図 3 8】 上記実施の形態 5 によるデータ管理システムのコンテンツを再生する際の暗号アルゴリズムによる認証を行う際の全体的な動作を説明するための図である。

【図 3 9】 上記実施の形態 5 によるデータ管理システムの認証を行う手順であるステップ G 1 の詳細な工程を示す図である。

【図 4 0】 上記実施の形態 5 によるデータ管理システムの認証を行う手順であるステップ G 2 の詳細な工程を示す図である。

【図 4 1】 上記実施の形態 5 によるデータ管理システムの認証を行う手順であるステップ G 3 の詳細な工程を示す図である。

【図 4 2】 上記実施の形態 5 によるデータ管理システムの認証を行う手順であるステップ G 4 の詳細な工程を示す図である。

【図 4 3】 上記実施の形態 5 によるデータ管理システムの認証を行う手順であるステップ G 5 の詳細な工程を示す図である。

【図 4 4】 従来のデータ管理システムによる著作権保護方式の一例である、CGMS (Copy Generation Management System) 方式を説明するための図である。

【図 4 5】 従来のデータ記憶媒体を用いたデータ管理システムの全体的な構成を示す構成図である。

【符号の説明】

- 90 センタホール
- 100 ディスクメディア
- 101a~101d 半導体チップ
- 102 データ領域
- 103 クリッピング領域
- 104 TOB (Table of contents) 領域
- 105 ワイヤ配線
- 106 トレイ
- 107 クリッピング

- 1 0 8 ワイヤ配線
- 1 0 9 スピンドルモータ
- 1 1 0 I/O
- 1 1 1 CPU
- 1 1 2 記憶部
- 1 1 4 タイトル
- 1 1 5 復号鍵部
- 1 1 6 デジタル出力制限回数情報
- 1 1 7 個人情報保持部
- 1 1 8 不正回数保持部
- 1 1 9 暗号部
- 1 2 0 乱数部
- 1 2 1 記憶部
- 2 0 0, 3 0 0, 4 0 0 記録再生装置
- 2 0 1 暗号部
- 2 0 2 メディア管理部
- 2 0 3 CPU
- 2 0 4 デジタルインターフェイス
- 2 0 5 D/A変換器
- 2 0 6 ユーザ設定部
- 2 0 7 表示部
- 2 0 8 光ピックアップ
- 2 0 9 A/D変換器
- 2 1 0 暗号部
- 2 1 1 乱数部
- 2 1 2 外部記録再生装置
- 2 1 3 接続ケーブル
- 2 1 4 鍵ボックス部
- 3 0 1 デジタルインターフェイス (A)

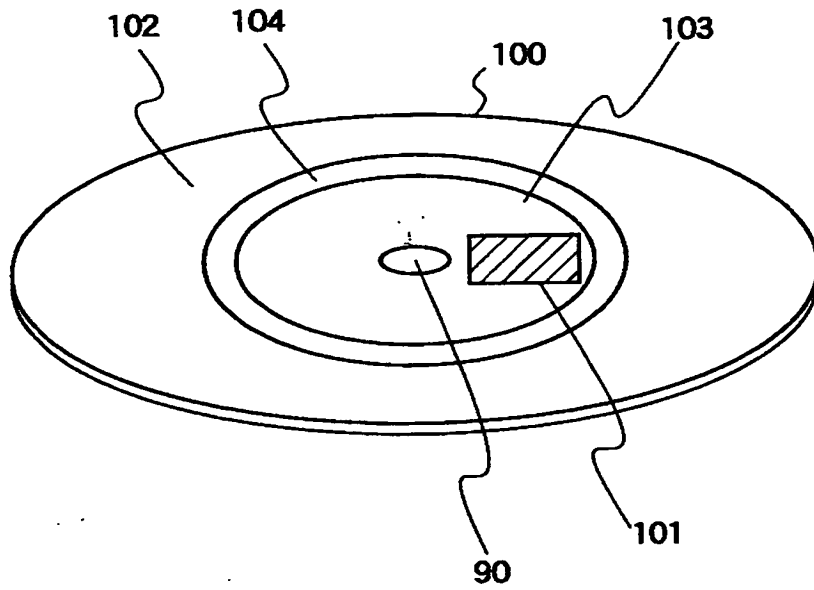
302 デジタルインターフェイス (B)

303 HDD装置 (A)

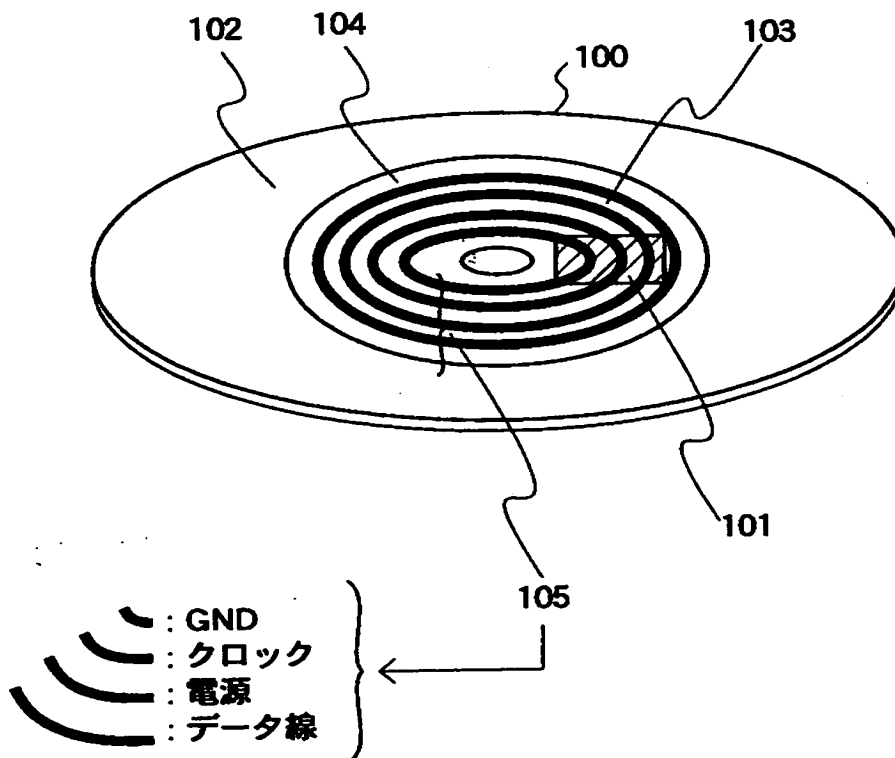
304 HDD装置 (B)

【書類名】 図面

【図 1】

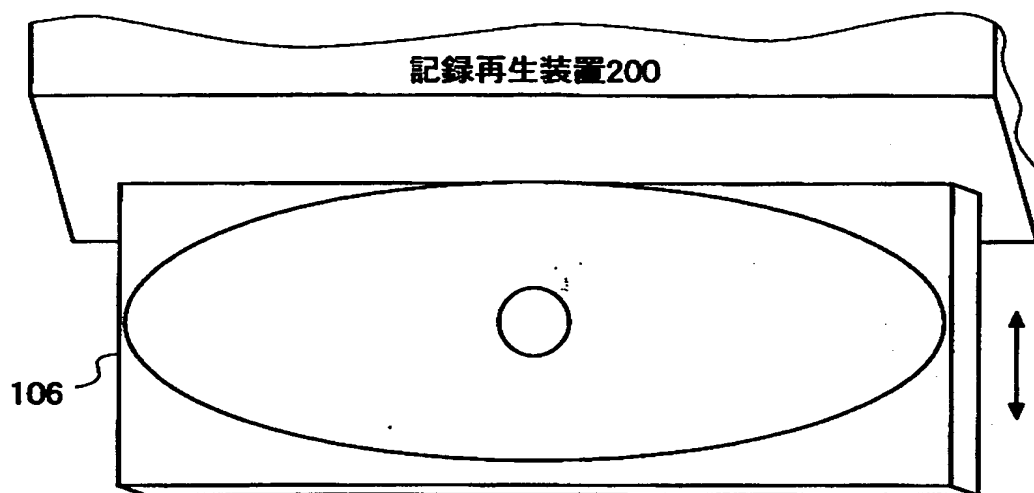


【図 2】

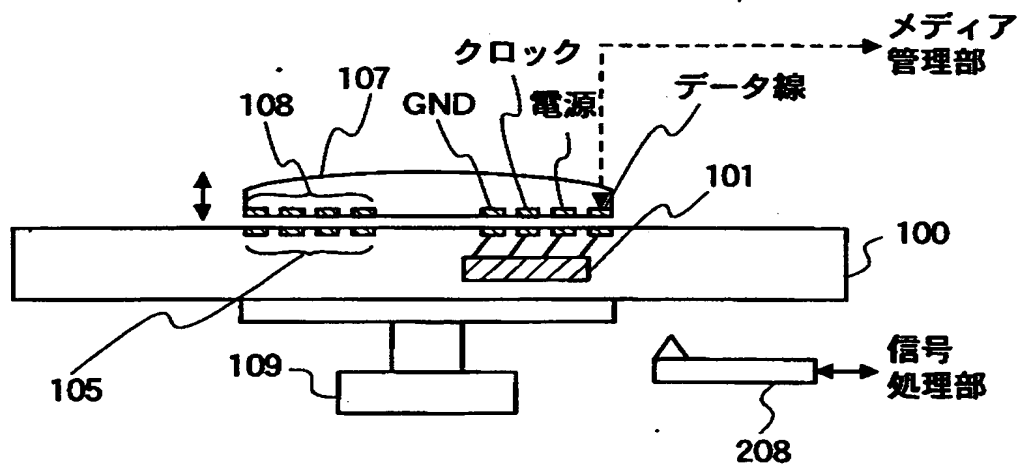


【図 3】

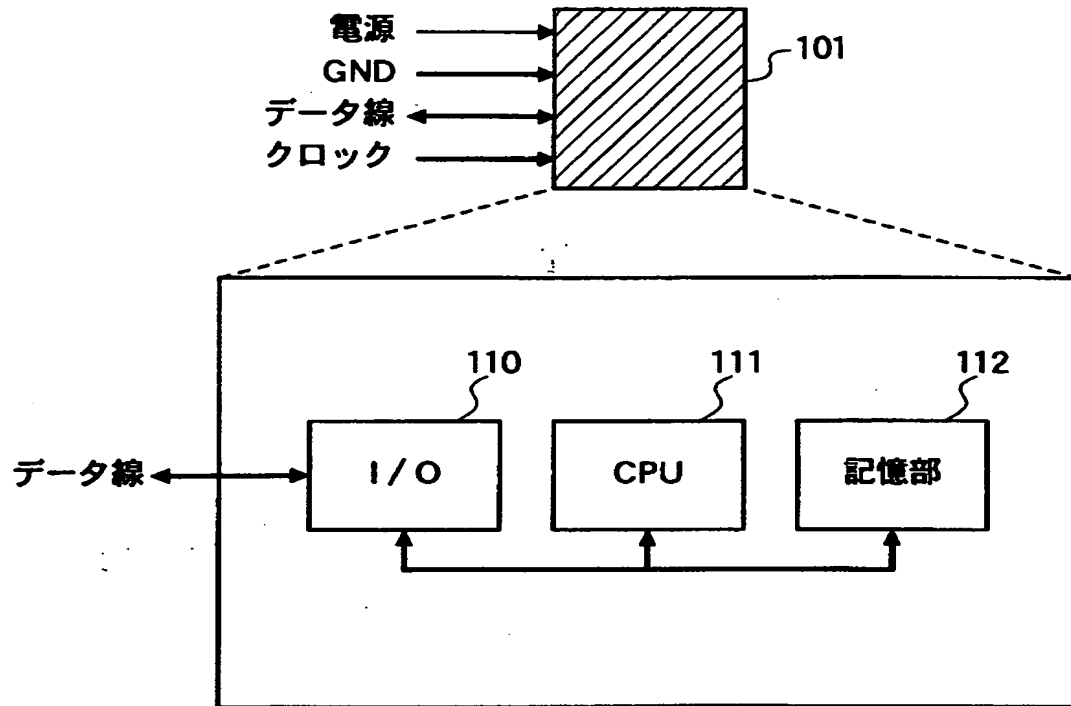
(a)



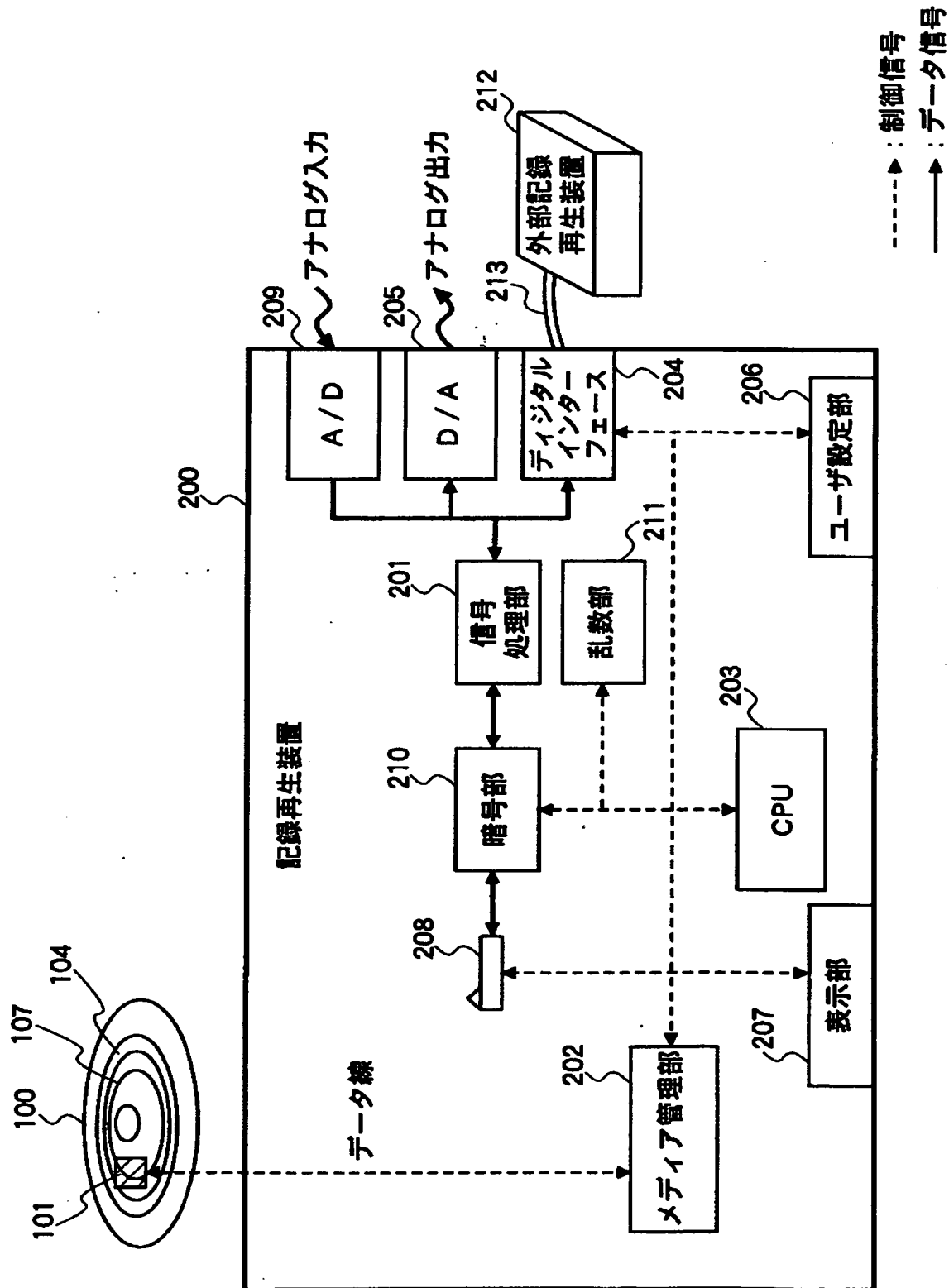
(b)



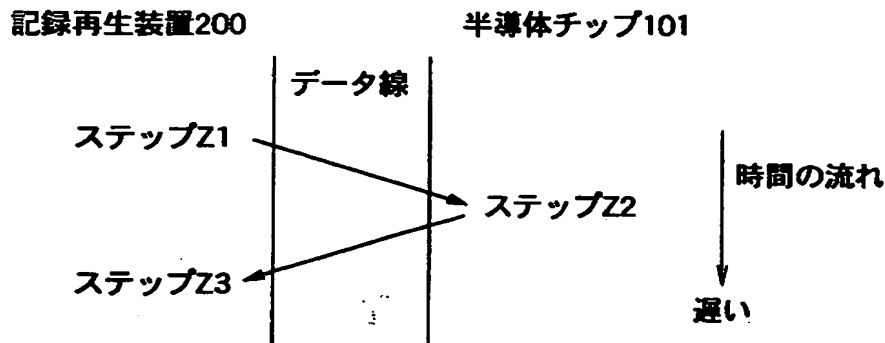
【図 4】



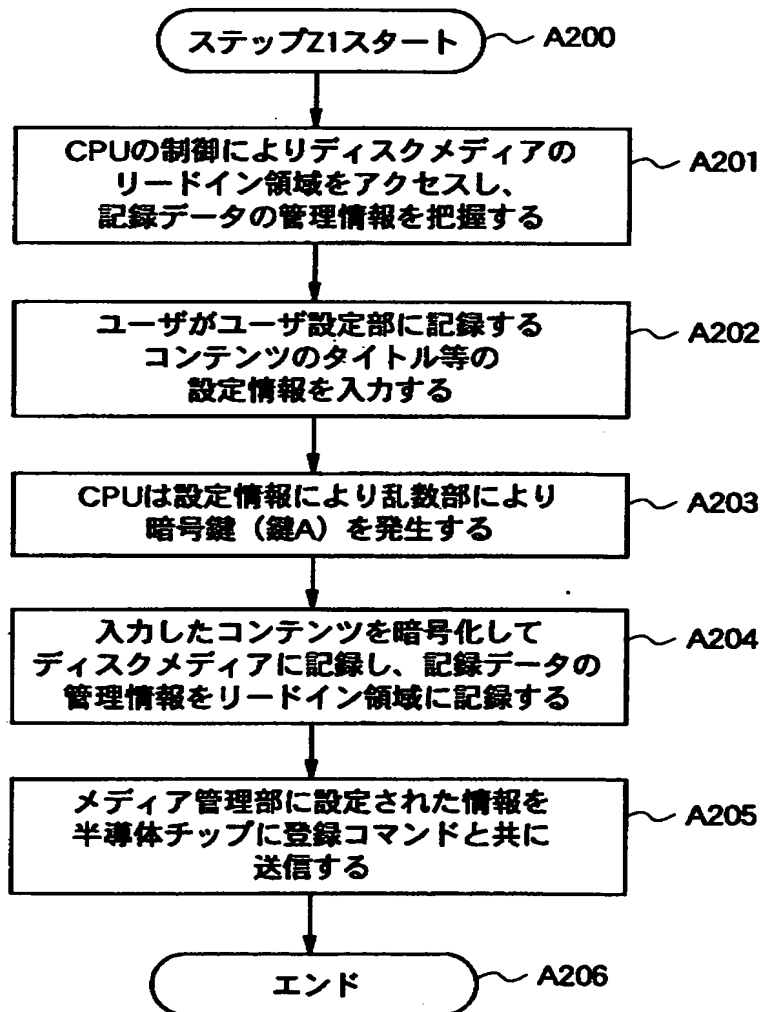
【図 5】



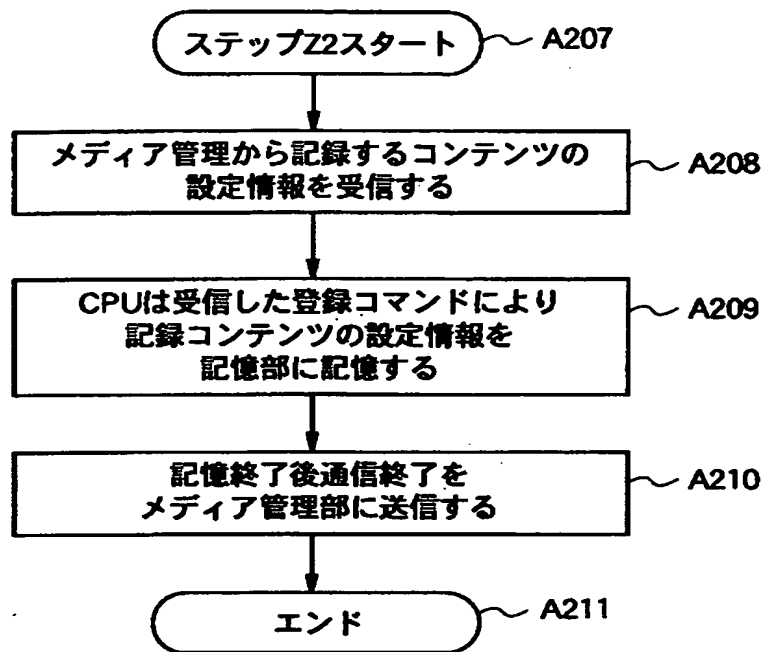
【図 6】



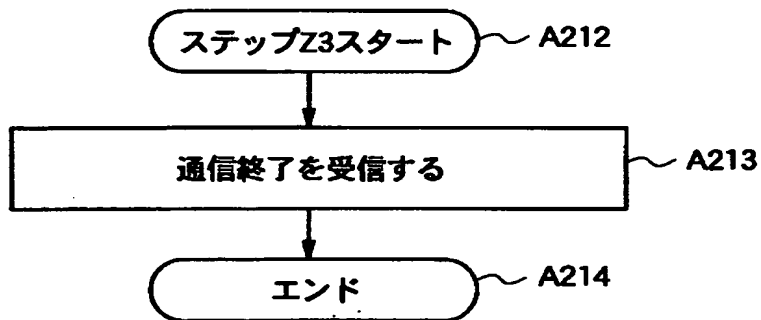
【図 7】



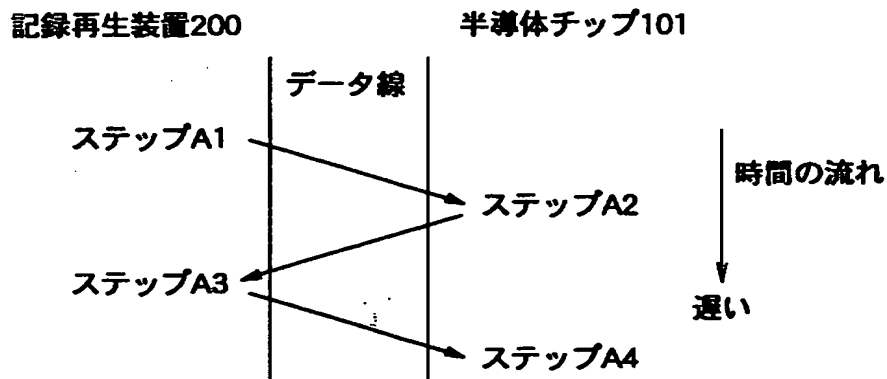
【図 8】



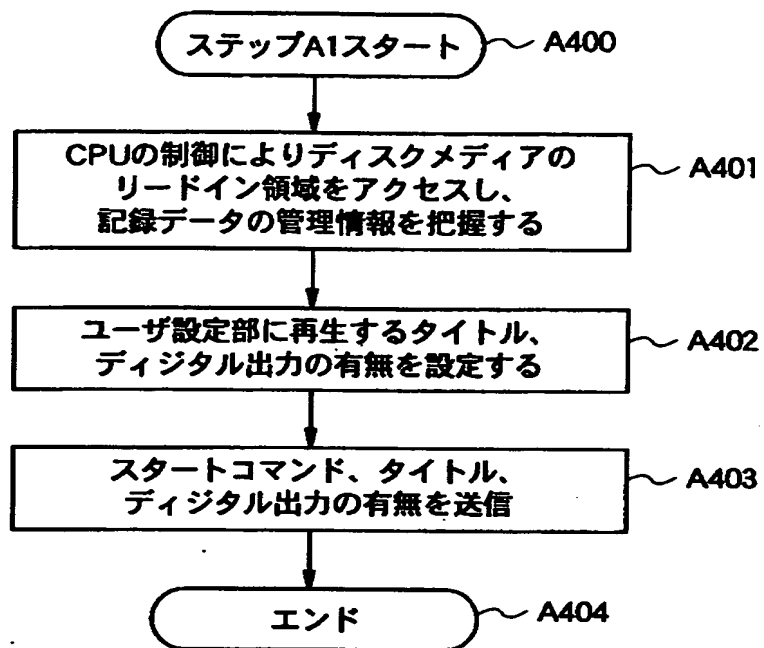
【図 9】



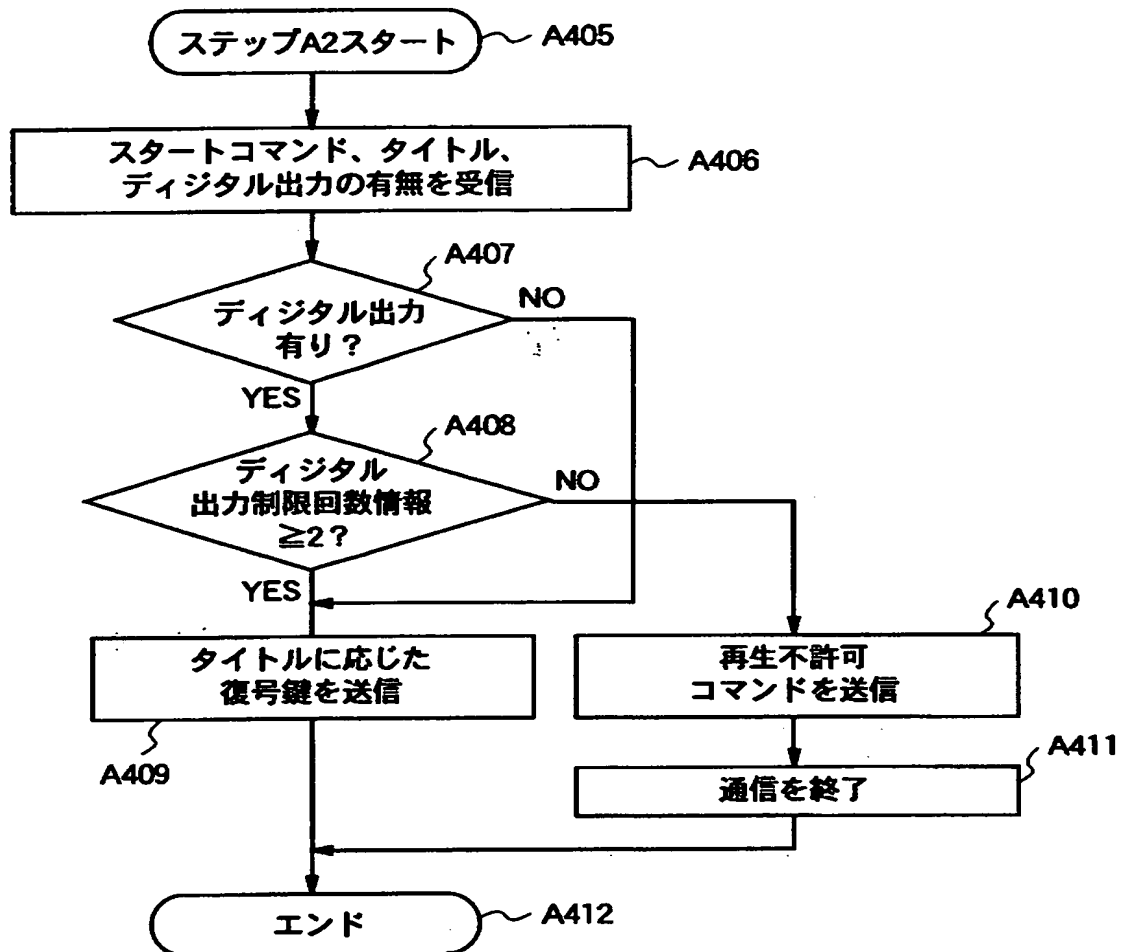
【図 10】



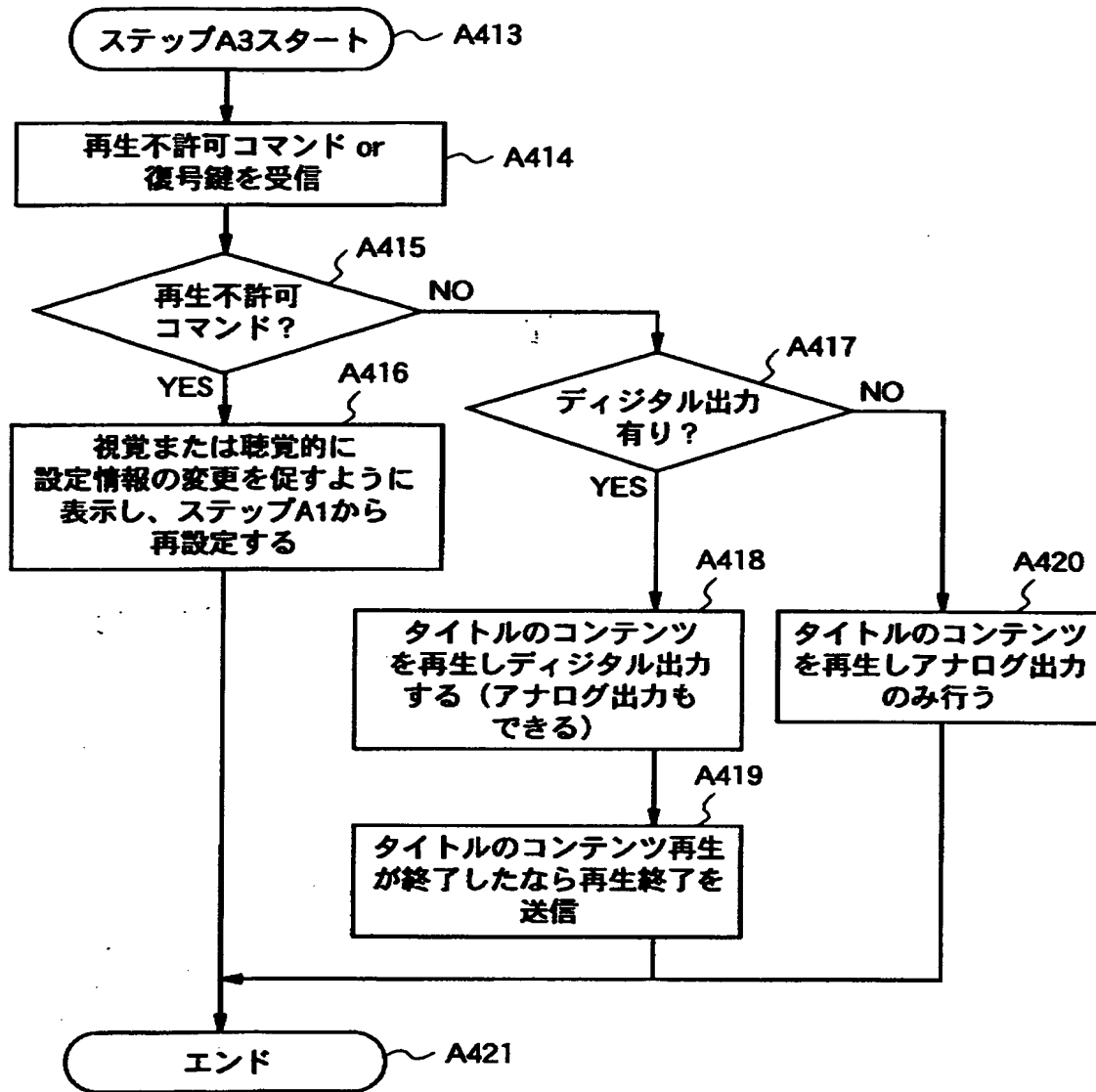
【図 11】



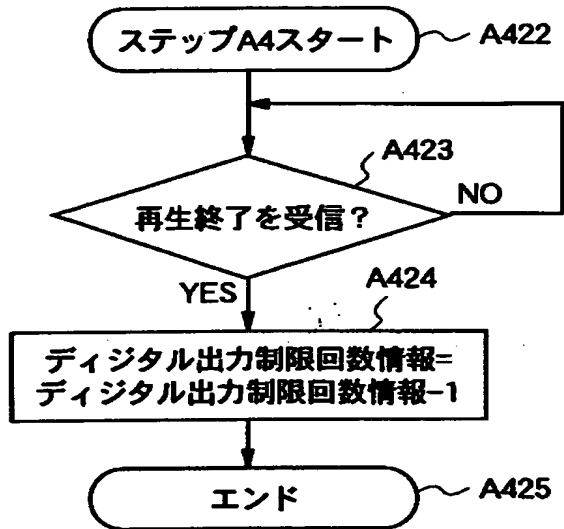
【図 12】



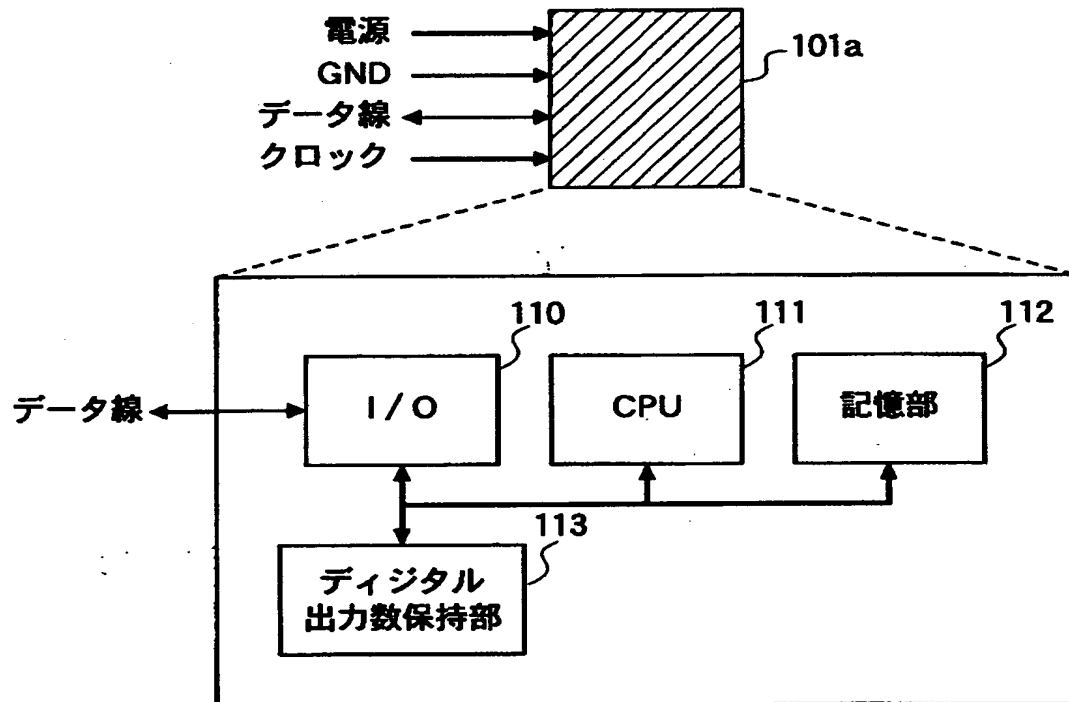
【図 13】



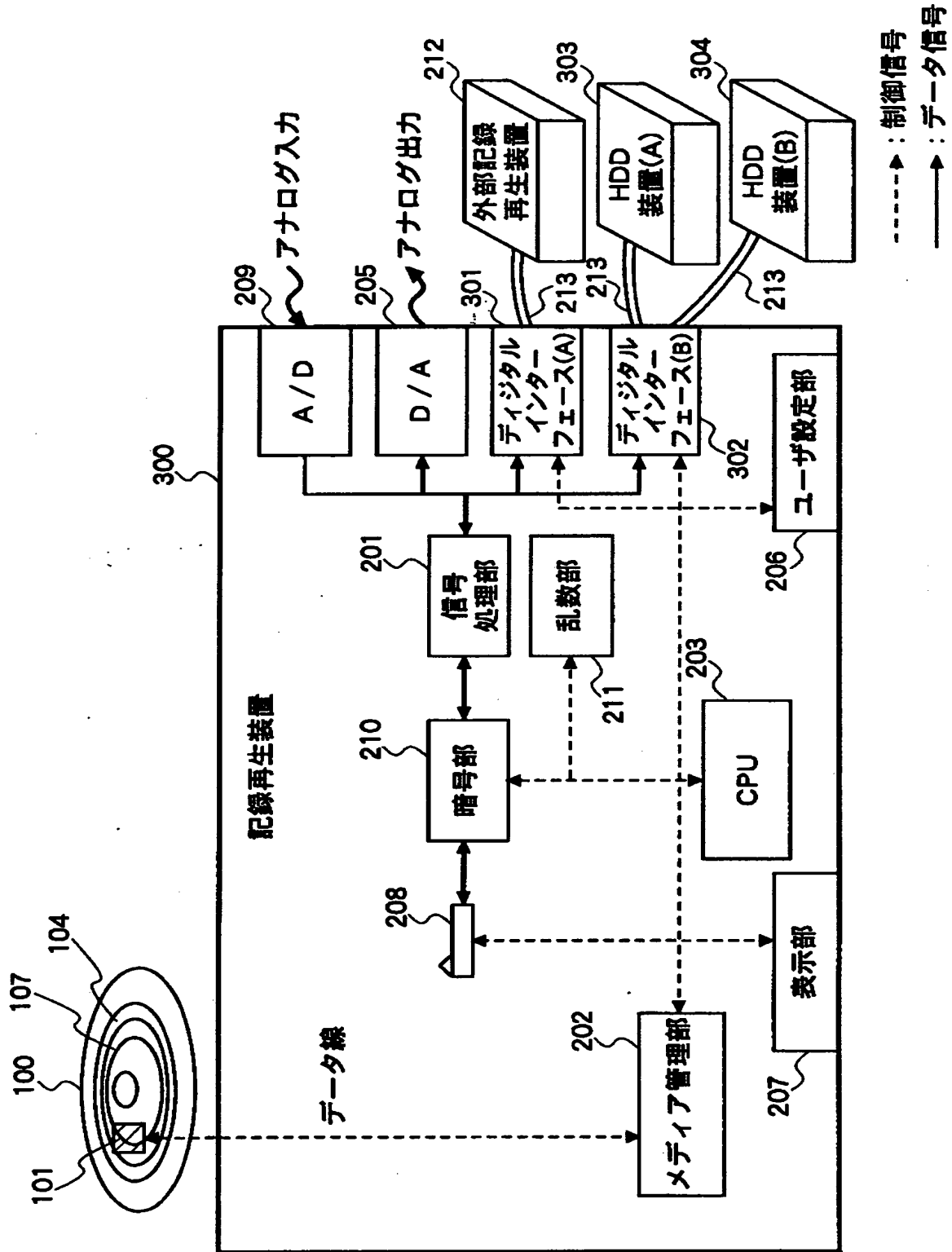
【図 1 4】



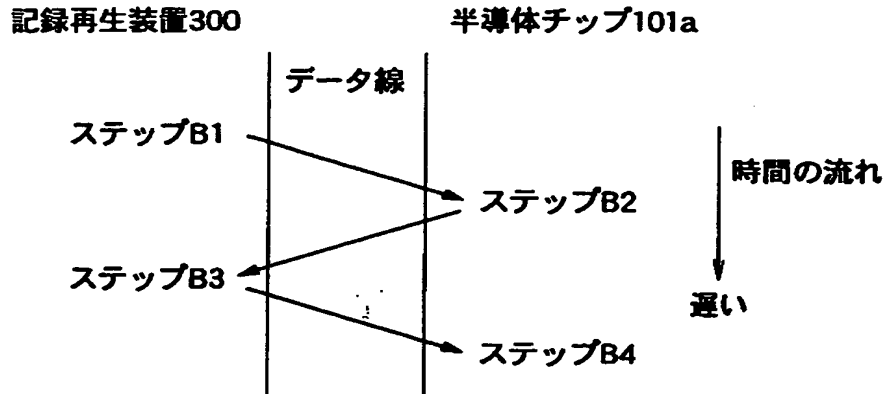
【図 1 5】



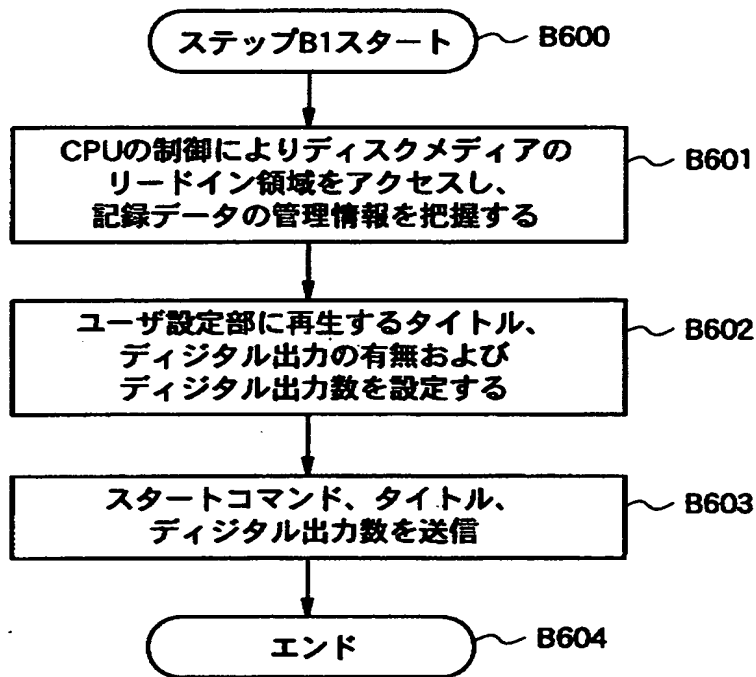
【図 16】



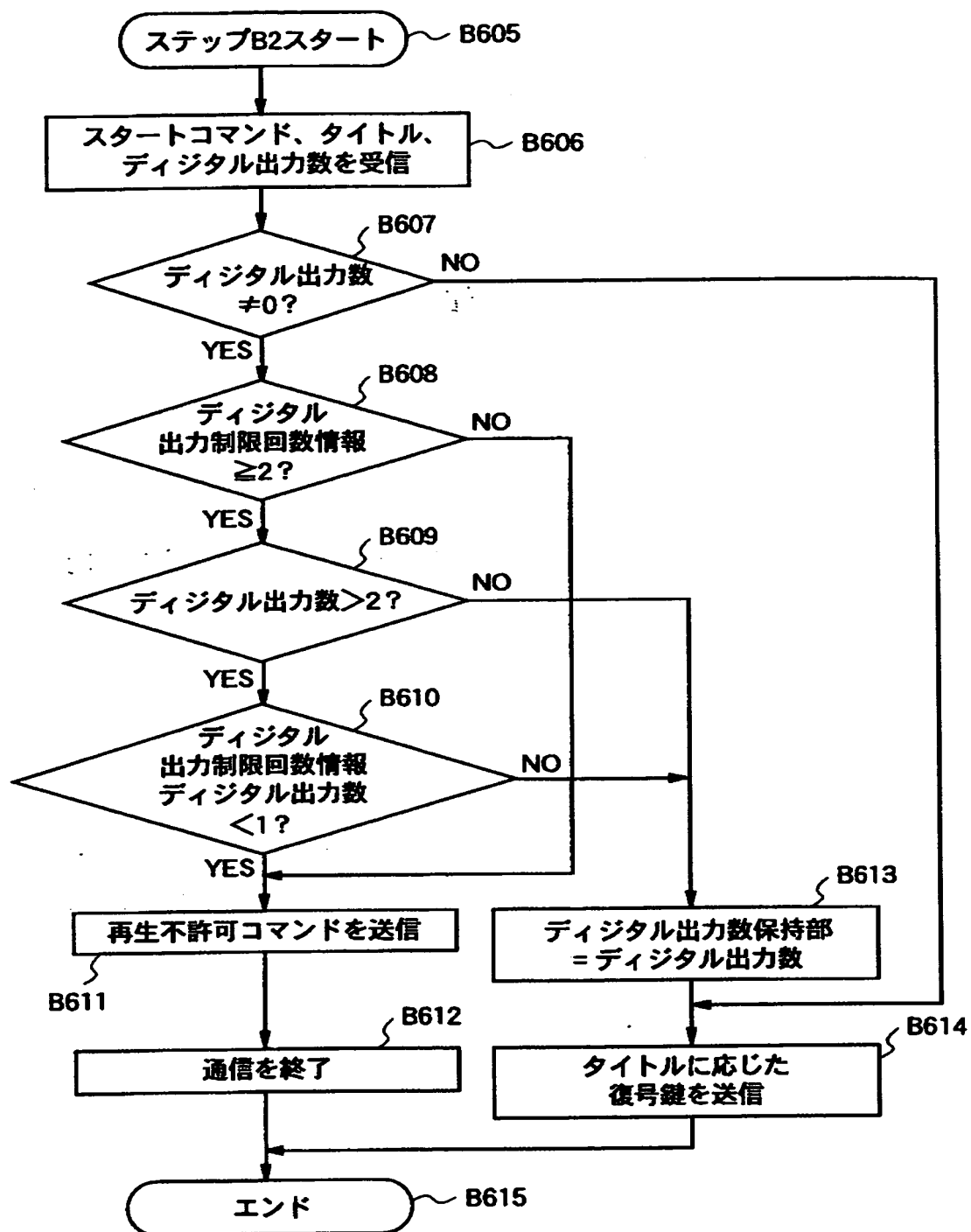
【図 1 7】



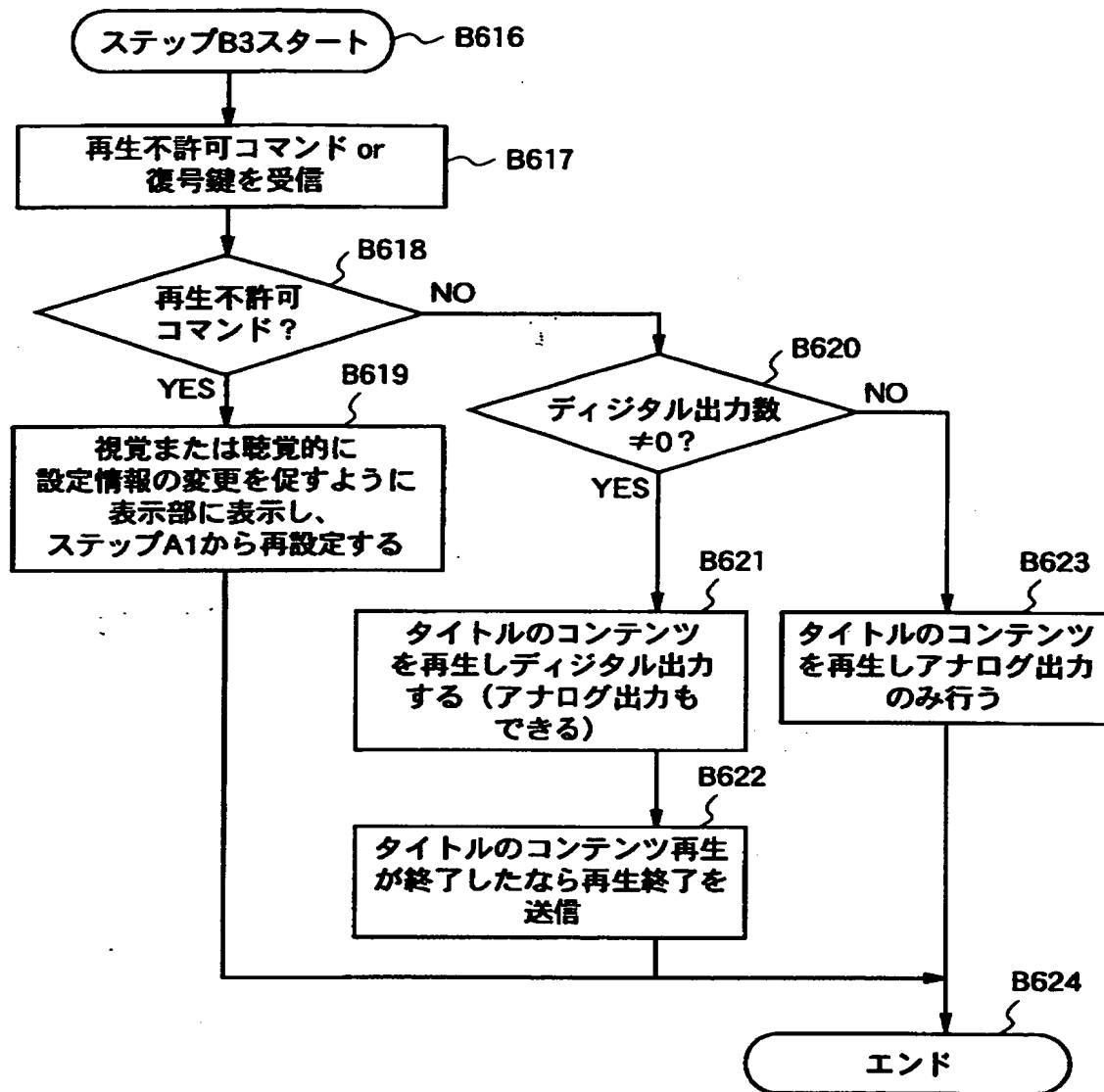
【図 1 8】



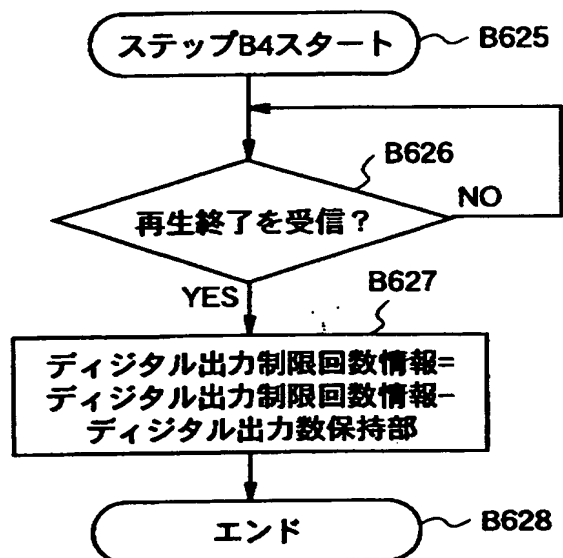
【図 1 9】



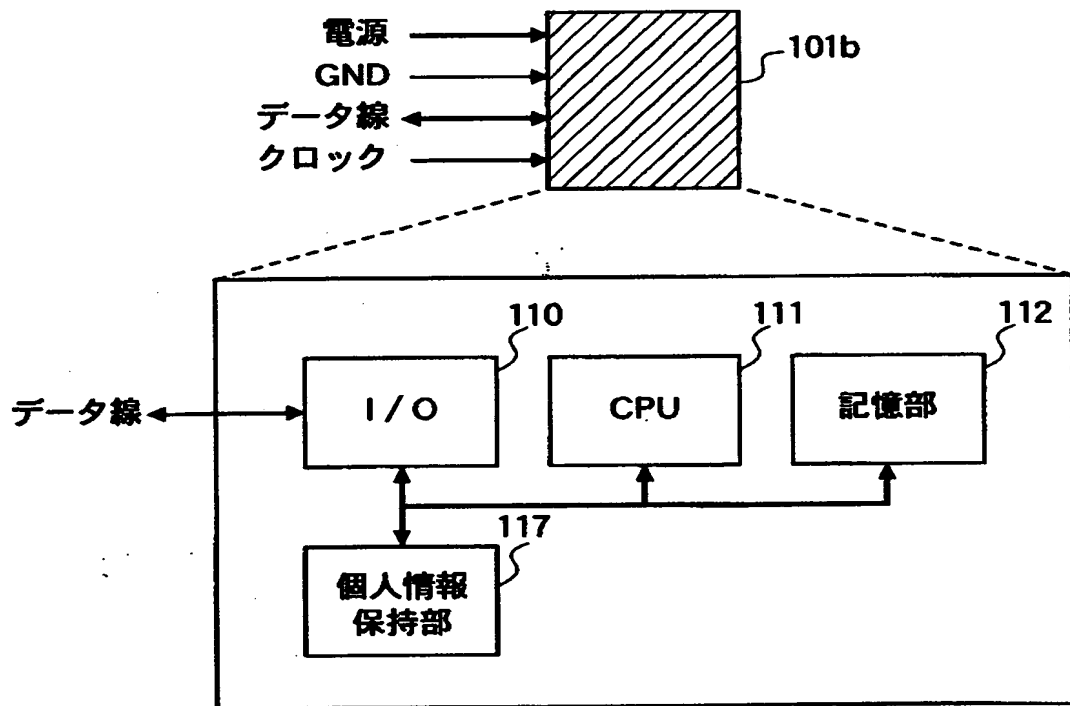
【図20】



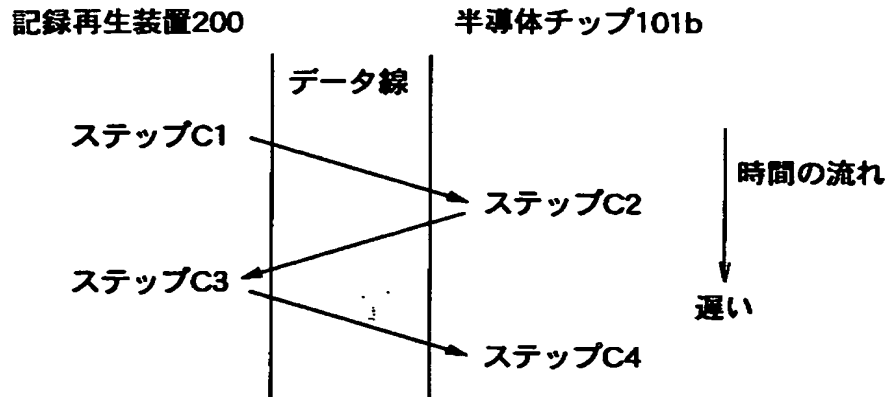
【図 2 1】



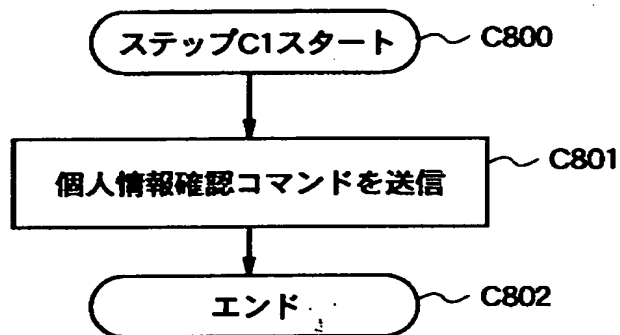
【図 2 2】



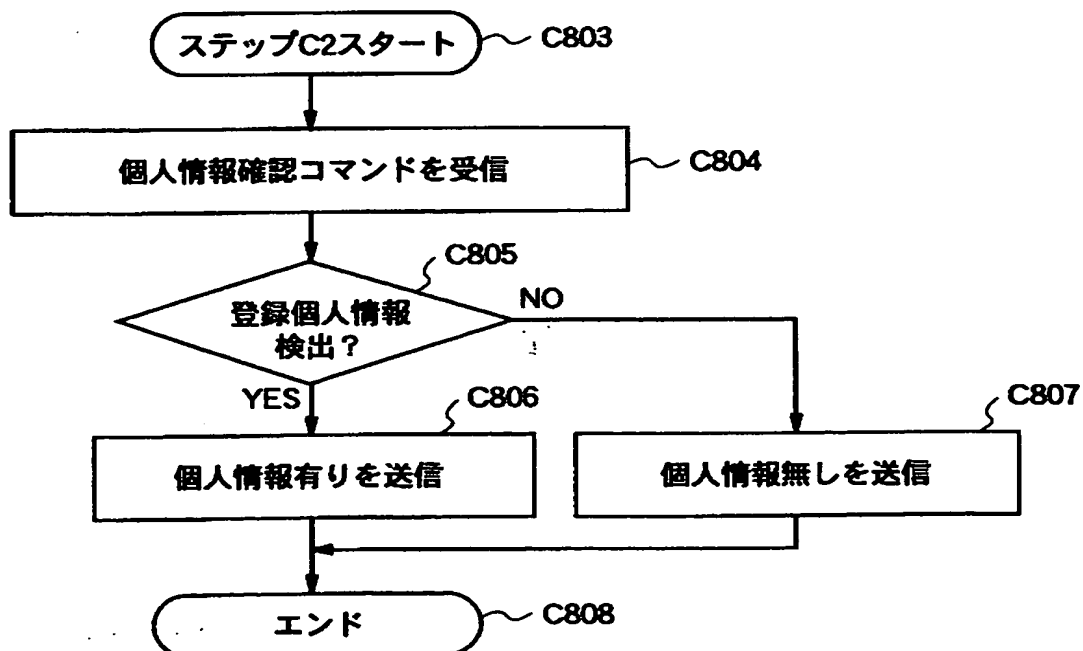
【図 23】



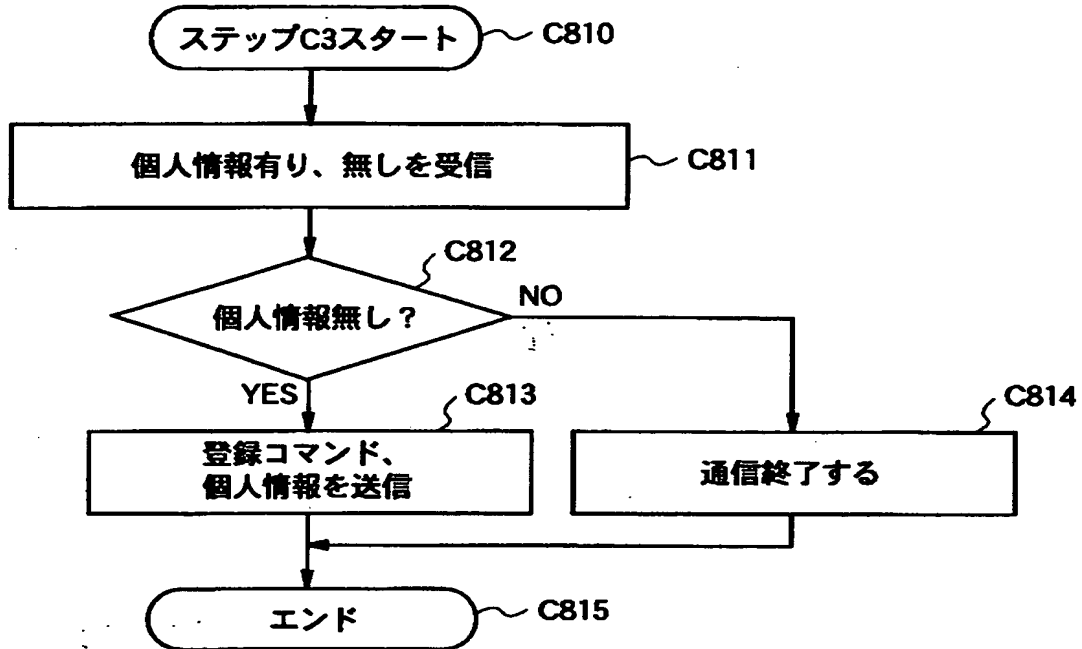
【図 24】



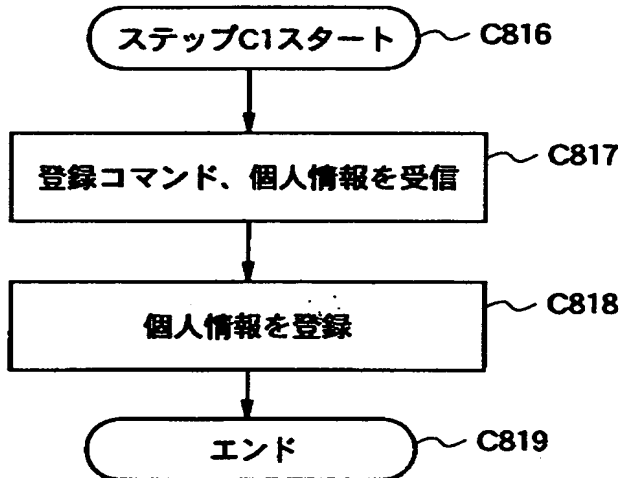
【図 25】



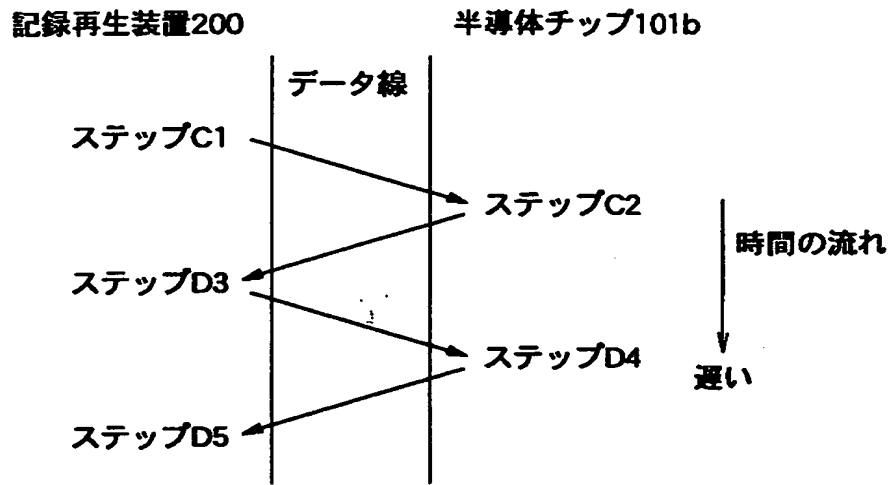
【図 26】



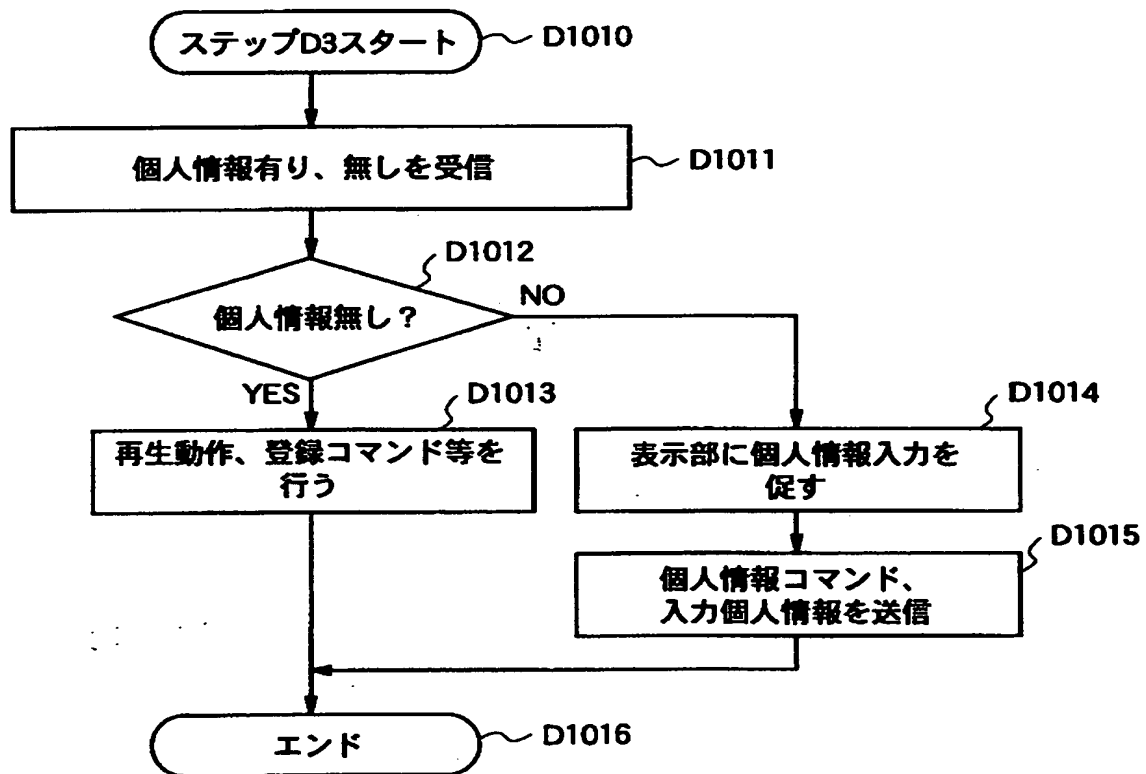
【図 27】



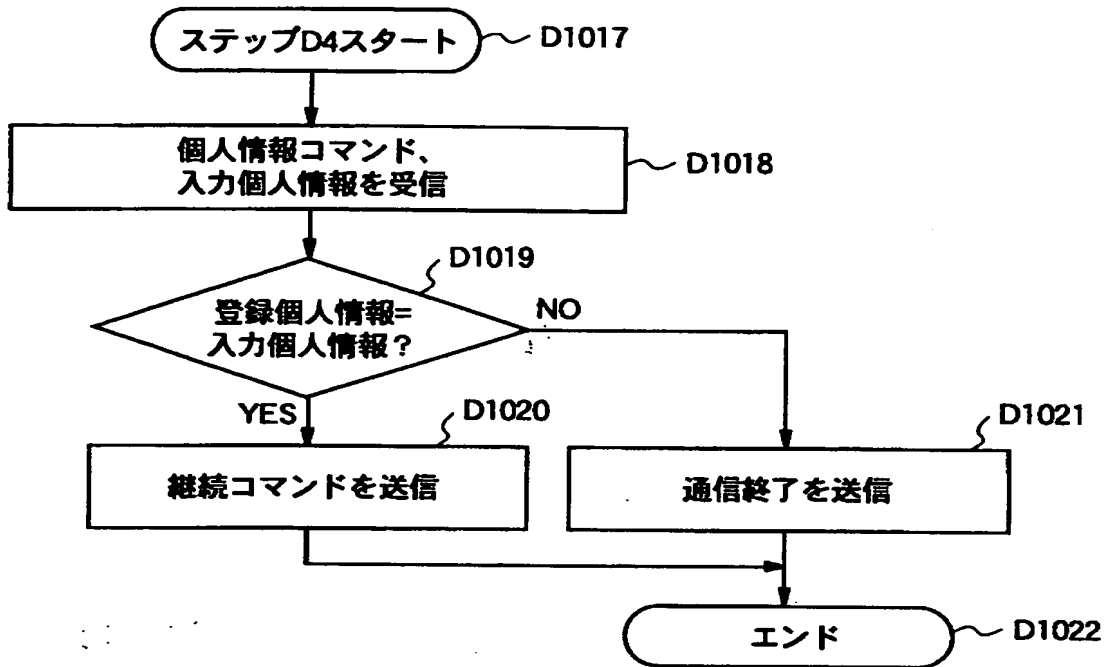
【図28】



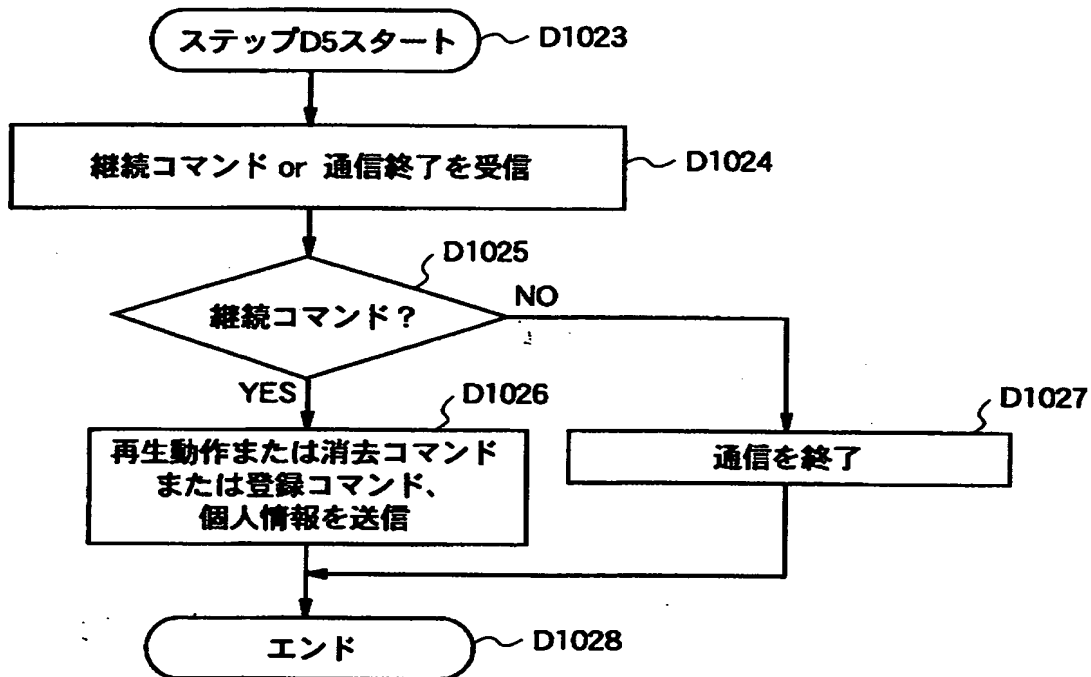
【図29】



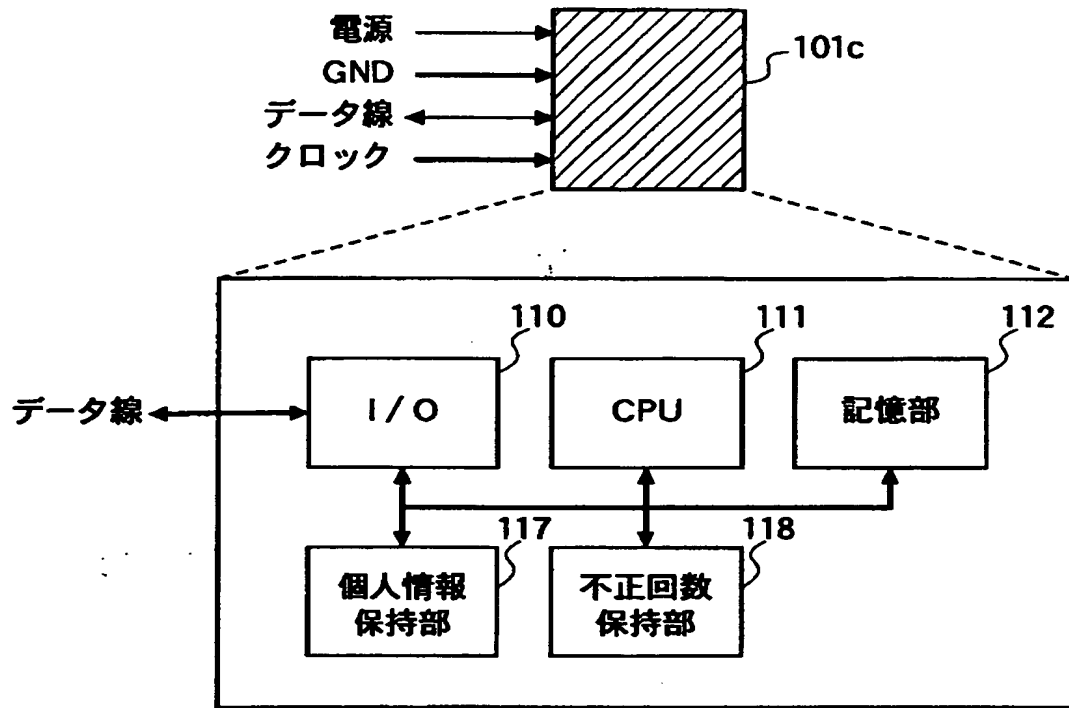
【図 30】



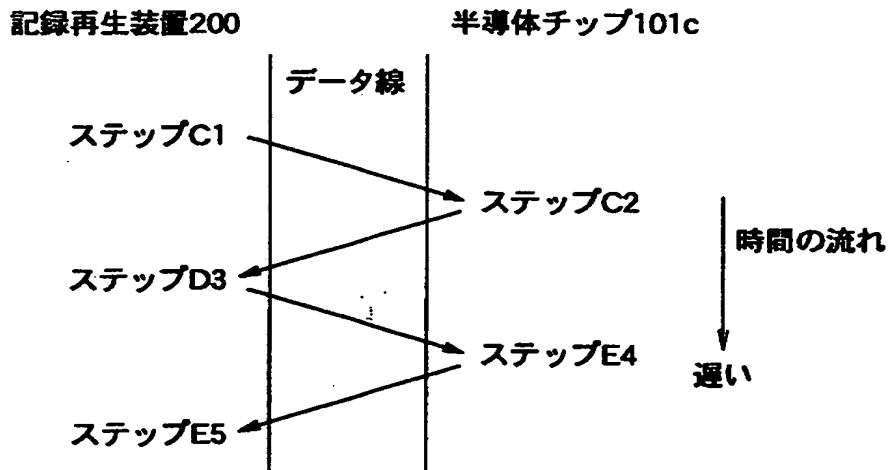
【図 31】



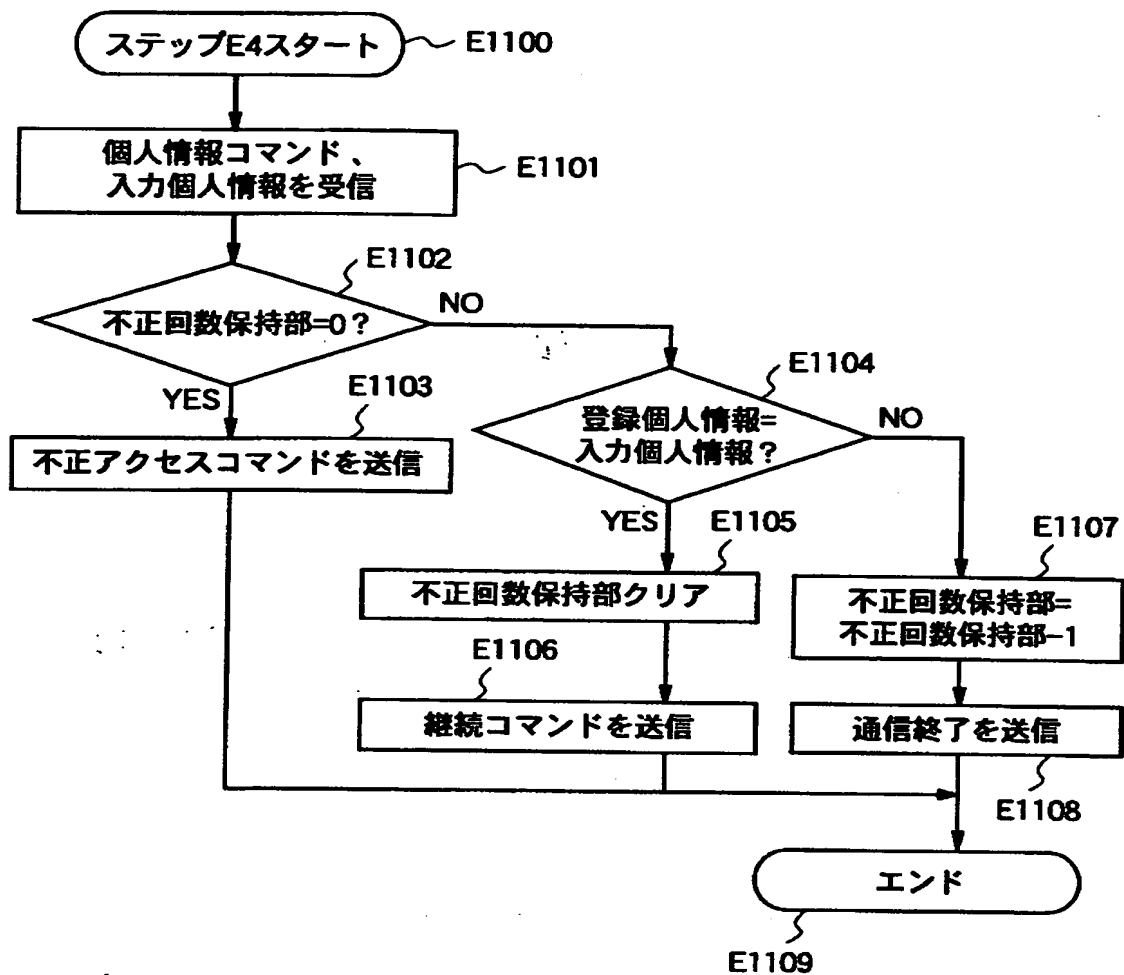
【図 3 2】



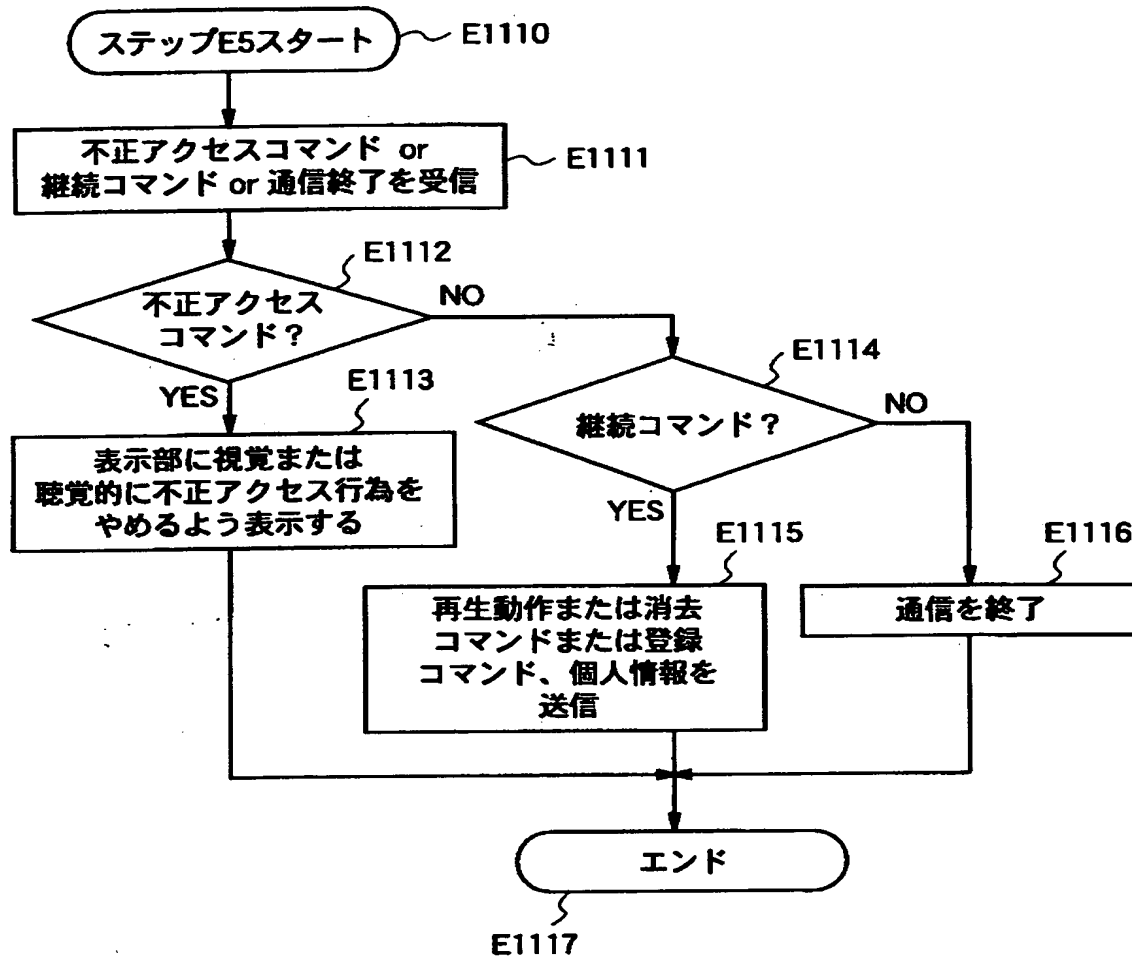
【図 3 3】



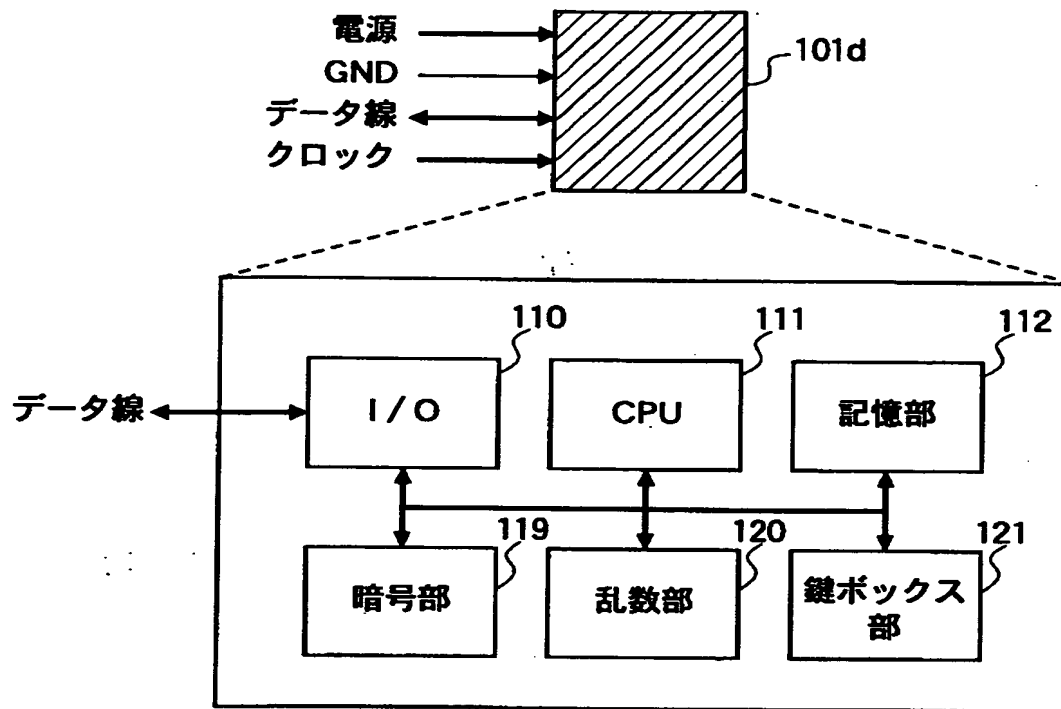
【図 3 4】



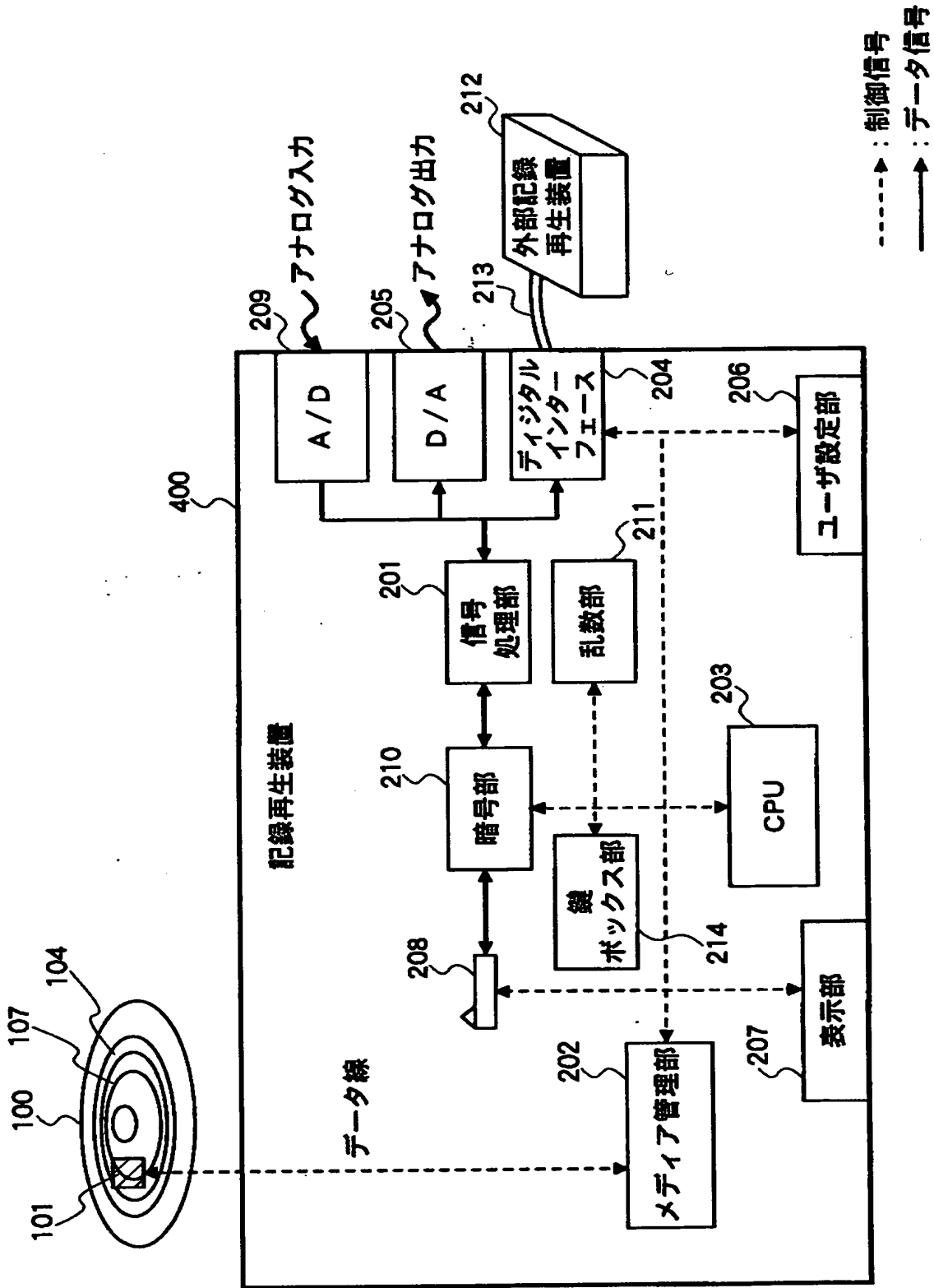
【図35】



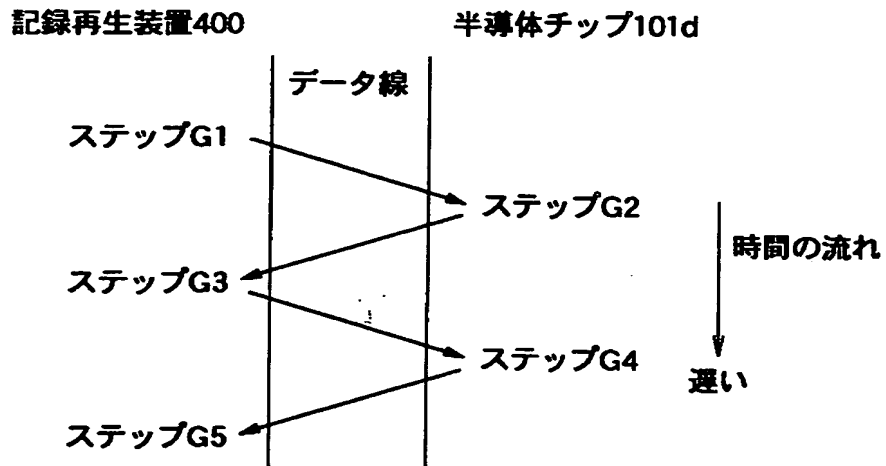
【図 3 6】



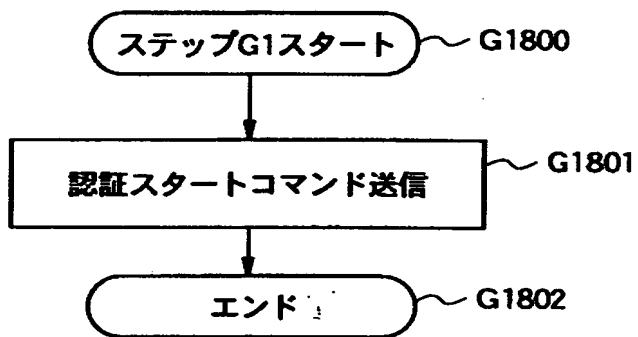
【図 37】



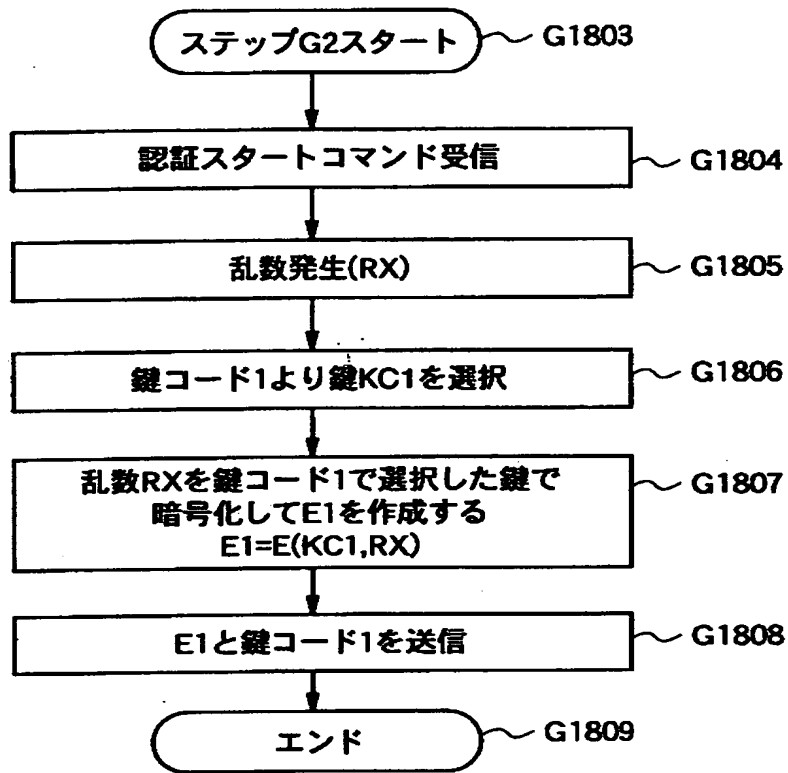
【図 3 8】



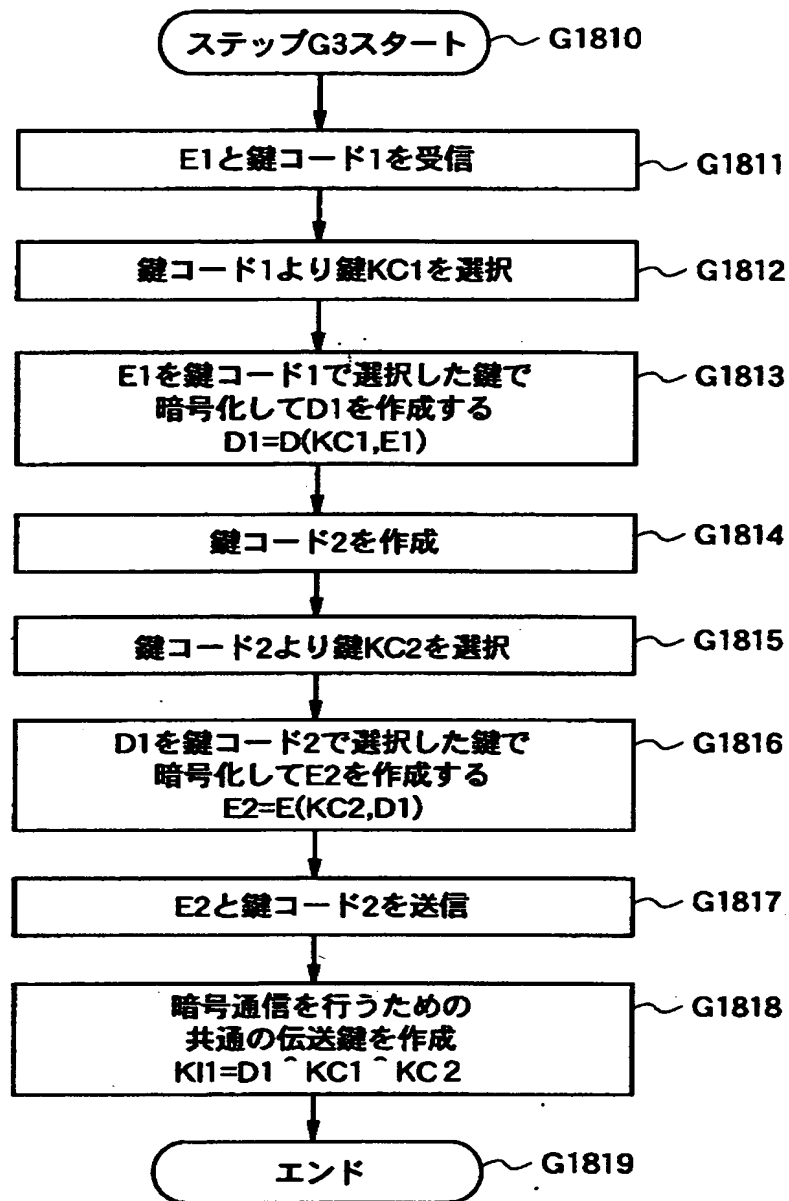
【図 3 9】



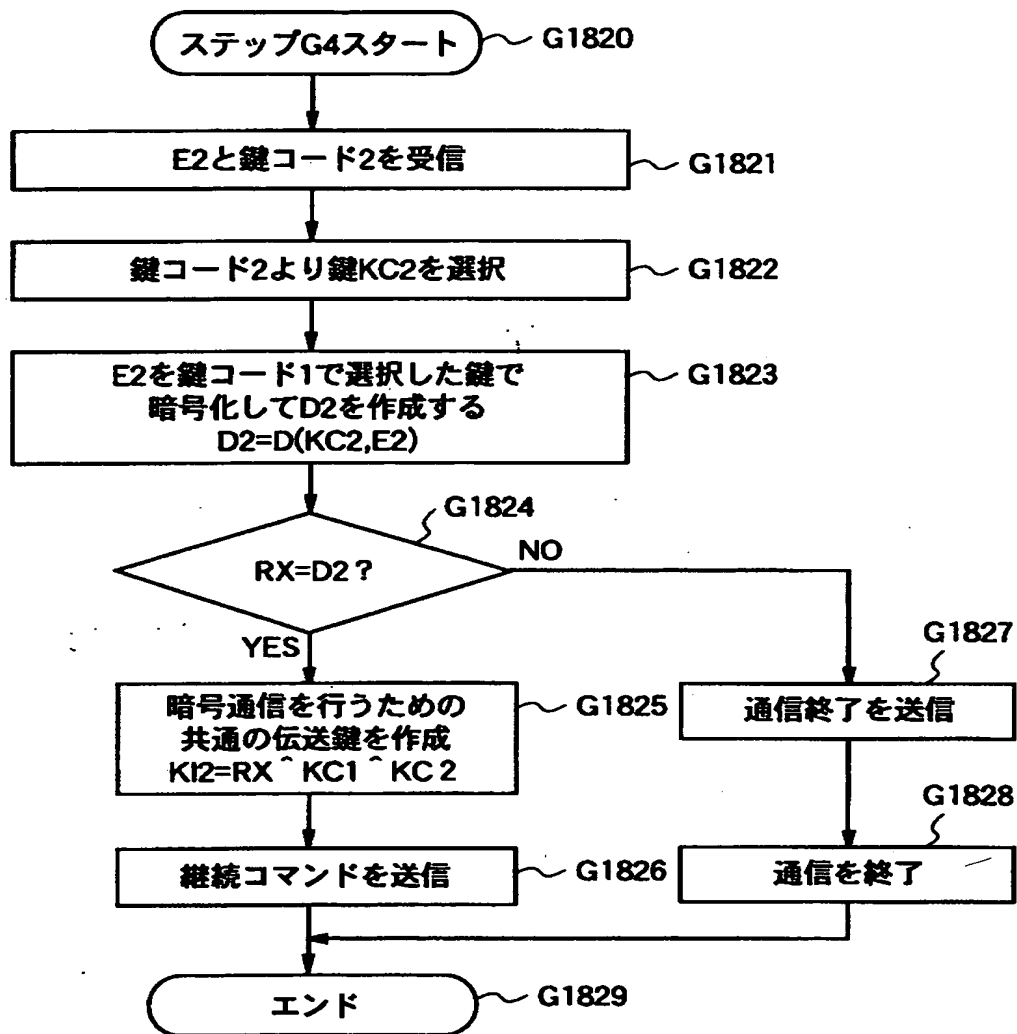
【図 40】



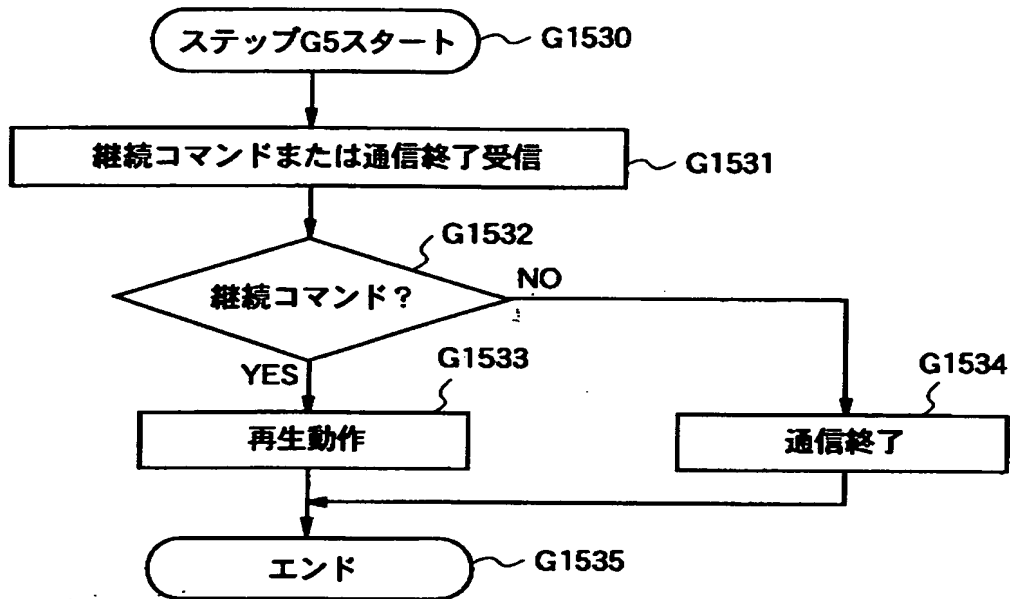
【図 4 1】



【図 4 2】



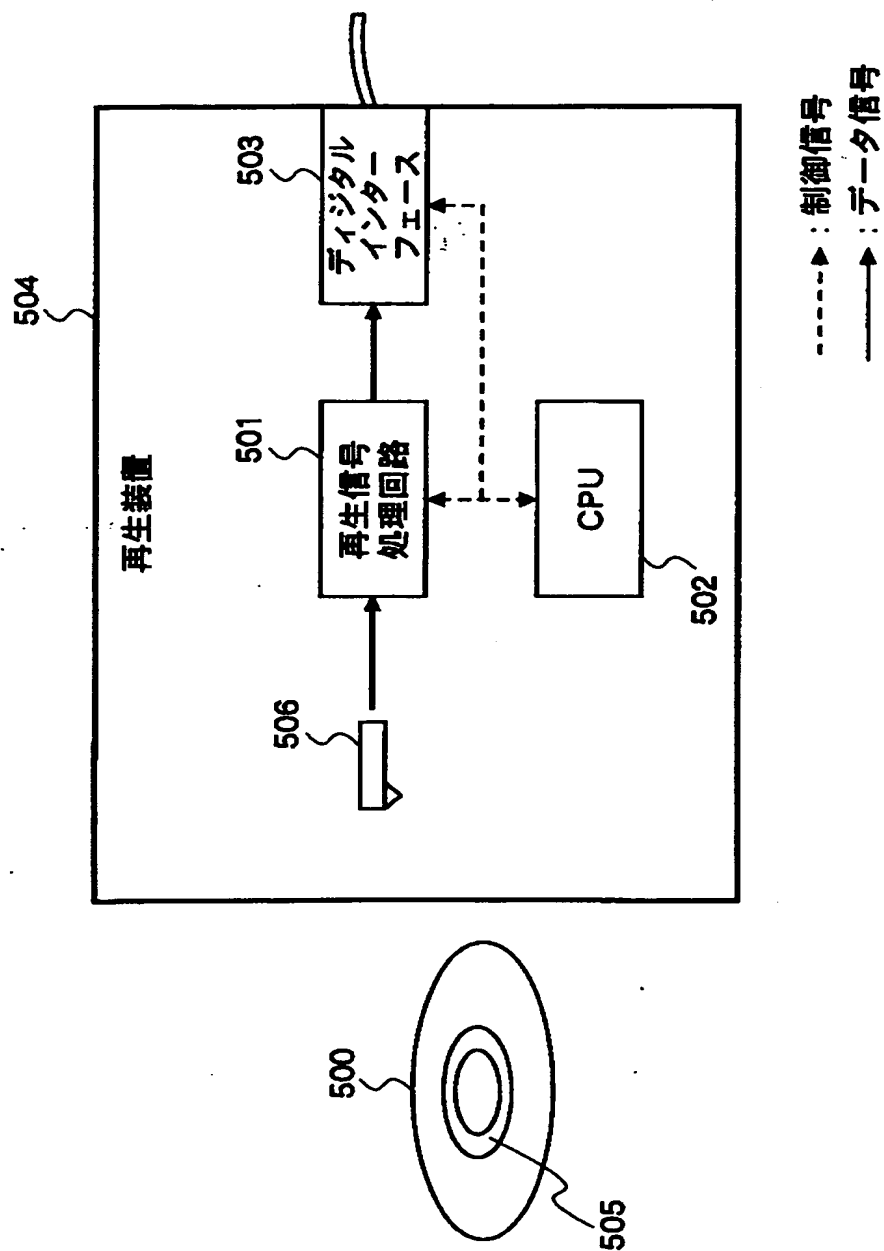
【図 4 3】



【図 4 4】

Free	コピー自由
Never Copy	コピー禁止
One More Copy	1回だけコピー可能
No More Copy	コピー禁止 (One More Copyのコンテンツを別のメディアに記録する際にNo More Copyする)

【図 45】



【書類名】 要約書

【要約】

【目的】 ディスクメディアのコンテンツ情報をデジタルコピーまたはデジタル出力する場合において、信頼性の高い著作権保護を提供すること。

【解決手段】 ディスクメディア 1 0 0 に内蔵した半導体 I C 1 0 1 を用いて、ディスクメディア 1 0 0 におけるコンテンツの再生を管理することで、デジタルインターフェース 2 0 4 からのデジタル出力を制限する。

【選択図】 図 5

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日

[変更理由] 新規登録

住 所 大阪府門真市大字門真1006番地

氏 名 松下電器産業株式会社

This Page Blank (uspto)